Red Hat Network Satellite 5.5 User Guide

Use and administration of Red Hat Network Satellite
Edition 2

Landmann

Red Hat Network Satellite 5.5 User Guide

Use and administration of Red Hat Network Satellite
Edition 2

Landmann
rlandmann@redhat.com

Legal Notice

Copyright © 2011 Red Hat, Inc.

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

This book covers use and operation of Red Hat Network Satellite. For further information, see the Red Hat Network Satellite Getting Started Guide.

Table of Contents

Preface 4

Chapter 1. User Administration 5
1.1. Adding, Deactivating, and Deleting User Accounts 5
1.2. User Management 9

Chapter 2. Automatic Synchronization 11

Chapter 3. Backup and Restore 12
3.1. Backups 12
3.2. Restore from Backup 13
3.3. Automated Backups 14

Chapter 4. Cloning a Machine 16
4.1. Features 16
4.2. Command Line Options 16
4.3. Example Usage 18

Chapter 5. Monitoring 19

Chapter 6. OpenSCAP 20
6.1. OpenSCAP Features 20
6.2. OpenSCAP in RHN Satellite 20
6.2.1. Prerequisites 21
6.2.2. Performing Audit Scans 21
6.2.3. How to View SCAP Results 24
6.2.4. OpenSCAP Satellite Pages 24
6.2.4.1. Audit 24
6.2.4.2. Systems → System Details → Audit 27

Chapter 7. PAM Authentication 31

Chapter 8. RPMs 33

Chapter 9. Boot Devices 36

Chapter 10. Organizations 41
10.1. Creating Organizations 42
10.2. Managing Entitlements 43
10.3. Configuring Systems in an Organization 44
10.4. Users of an Organization 45
10.5. Organizational Trusts 45

Revision History 49

Index 51
A 51
C 51
D 51
E 51
F 52
O 52
P 52
S 52

U 52
W 52

Preface

Red Hat Network provides system-level support and management of Red Hat systems and networks. It brings together the tools, services, and information repositories needed to maximize the reliability, security, and performance of Red Hat systems. To use Red Hat Network system administrators register software and hardware profiles, known as System Profiles, of their client systems with Red Hat Network. When a client system requests package updates, only the applicable packages for the client are returned.

RHN Satellite Server Server allows organizations to use the benefits of Red Hat Network without having to provide public Internet access to their servers or other client systems. System profiles are stored locally on the Satellite Server. The Red Hat Network Satellite website is served from a local web server and is only accessible to systems that can reach the Satellite. All package management tasks, including errata updates, are performed through the Satellite server.

RHN Satellite Server Server provides a solution to organizations requiring absolute control over and privacy of the maintenance and package deployment of their servers. It allows Red Hat Network customers the greatest flexibility and power in keeping systems secure and updated. Modules can be added to the Satellite Server to allow extra functionality. This document provides guidance on operations which are essential when running Satellite Server.

Chapter 1. User Administration

1.1. Adding, Deactivating, and Deleting User Accounts

Users can be managed through the **Users** tab at the top of the RHN Satellite Server navigation bar. From this tab, user permissions can be granted and edited.

Procedure 1.1. Adding Users

To add new users to the organization:

1. In the **Users** tab, click **Create new user** to open the **Create User** page.

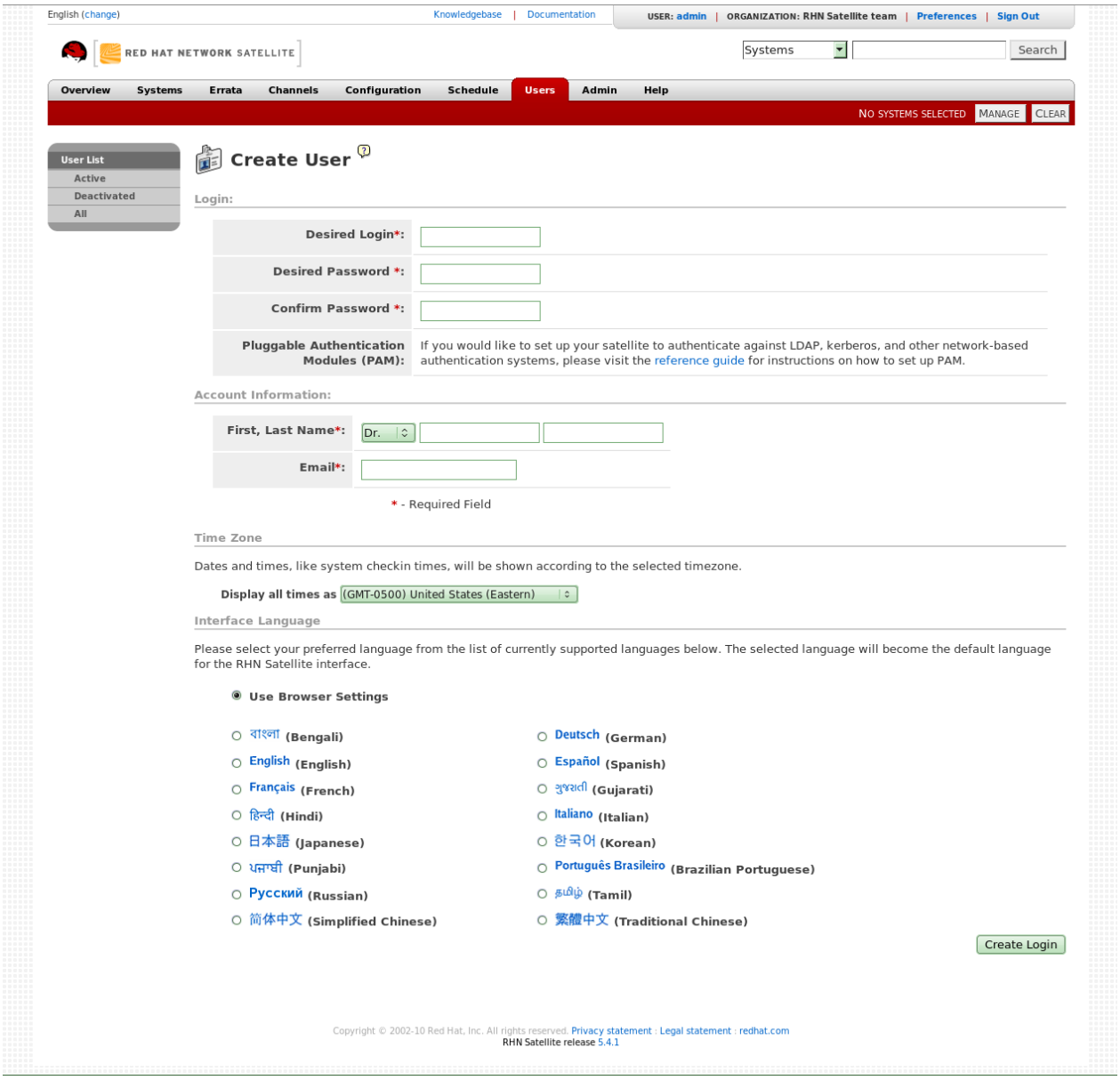
English (change)
Knowledgebase | Documentation
USER: admin | ORGANIZATION: RHN Satellite team | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Admin Help
NO SYSTEMS SELECTED MANAGE CLEAR
User List
Active
Deactivated
All
Create User
Login:
Desired Login*:
Desired Password *:
Confirm Password *:
Pluggable Authentication Modules (PAM):
If you would like to set up your satellite to authenticate against LDAP, kerberos, and other network-based authentication systems, please visit the reference guide for instructions on how to set up PAM.
Account Information:
First, Last Name*:
Dr.
Email*:
* - Required Field
Time Zone
Dates and times, like system checkin times, will be shown according to the selected timezone.
Display all times as (GMT-0500) United States (Eastern)
Interface Language
Please select your preferred language from the list of currently supported languages below. The selected language will become the default language for the RHN Satellite interface.
Use Browser Settings
বাংলা (Bengali)
English (English)
Français (French)
हिन्दी (Hindi)
日本語 (Japanese)
ਪੰਜਾਬੀ (Punjabi)
Русский (Russian)
简体中文 (Simplified Chinese)
Deutsch (German)
Español (Spanish)
ગુજરાતી (Gujarati)
Italiano (Italian)
한국어 (Korean)
Português Brasileiro (Brazilian Portuguese)
தமிழ் (Tamil)
繁體中文 (Traditional Chinese)
Create Login
Copyright © 2002-10 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
RHN Satellite release 5.4.1

Figure 1.1. The Create User page

2. In the **Desired Login** field, enter a name for the user. The login name must be at least five characters long.
3. In the **Desired Password** field, enter a password for the user. Re-enter the same password to

confirm.

4. In the **First, Last Name** field, enter a first and last name for the user. Select a suitable prefix (for example: Mr, Miss, Mrs) from the drop-down menu.
5. In the **Email** field, enter an email address for the user.
6. In the **Time Zone** section, select an appropriate time zone.
7. In the **Interface Language** section, select an appropriate language to be used in the RHN Satellite Server interface.
8. Click **Create Login** to create the new user. An email will be sent to the user (using the address specified during creation) to inform them of the new account details.
9. Once the account has been successfully created, you will be redirected to the **User List** page. To change permissions and set options for the new user, select their name from the displayed list to display the **User Details** page, and navigate to the appropriate tabs to make your changes.

Procedure 1.2. Deactivating Users

User accounts can be deactivated by administrators, or users can deactivate their own accounts. Deactivated user accounts are not able to be used to log in to the RHN Satellite Server interface, or schedule actions. Any actions that were scheduled before the account was deactivated will remain in the action queue until they are completed. Deactivated user accounts can be reactivated by administrators.

Administrator accounts can only be deactivated once the administrator role has been removed from the account.

To deactivate a user account:

1. Select the user's name from the list in the **Users** tab, to display the **User Details** page.
2. Check to see if the user is a Satellite administrator.

   If the user is a Satellite administrator, uncheck the box next to that role, and click **Submit**.

   If the user is not a Satellite administrator, continue to the next step.
3. Click **Deactivate User**.

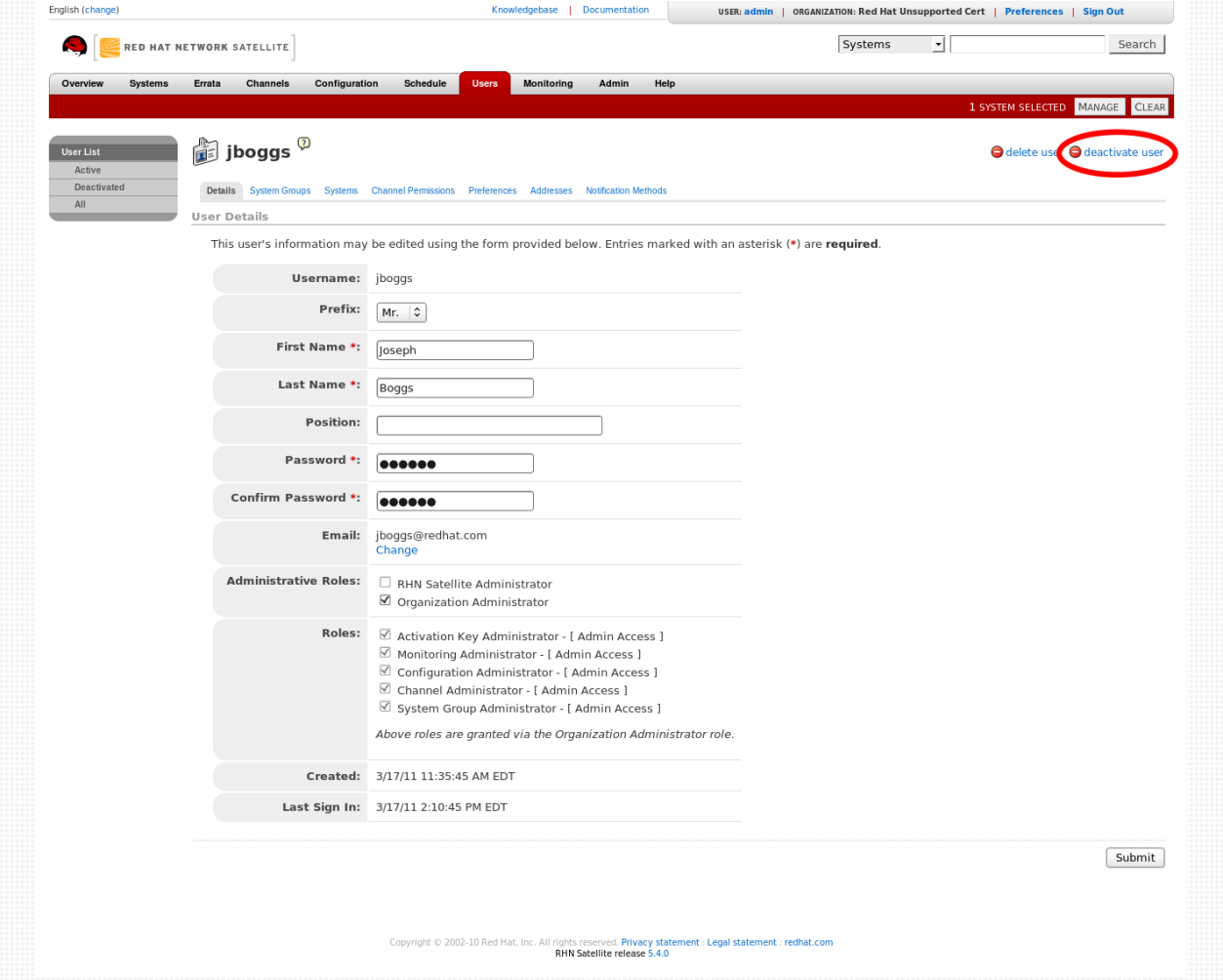
English (change)
Knowledgebase | Documentation
USER: admin | ORGANIZATION: Red Hat Unsupported Cert | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Monitoring Admin Help
1 SYSTEM SELECTED MANAGE CLEAR
User List
Active
Deactivated
All
jboggs
delete user
deactivate user
Details System Groups Systems Channel Permissions Preferences Addresses Notification Methods
User Details
This user's information may be edited using the form provided below. Entries marked with an asterisk (*) are required.
Username: jboggs
Prefix: Mr.
First Name *: joseph
Last Name *: Boggs
Position:
Password *:
Confirm Password *:
Email: jboggs@redhat.com
Change
Administrative Roles:
RHN Satellite Administrator
Organization Administrator
Roles:
Activation Key Administrator - [Admin Access]
Monitoring Administrator - [Admin Access]
Configuration Administrator - [Admin Access]
Channel Administrator - [Admin Access]
System Group Administrator - [Admin Access]
Above roles are granted via the Organization Administrator role.
Created: 3/17/11 11:35:45 AM EDT
Last Sign In: 3/17/11 2:10:45 PM EDT
Submit
Copyright © 2002-10 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
RHN Satellite release 5.4.0

Figure 1.2. Deactivating users

You will be asked to confirm this action, by clicking it again. Check the details, and then click **`Deactivate User`** again to confirm.

4. Once the account has been successfully deactivated, the user's name will not appear in the **`Active Users`** list. Click the **`Deactivated`** link from the **`User List`** menu to view deactivated user accounts.
5. To reactivate the user account, view the **`Deactivated`** list, check the box next to the user to be reactivate, and click **`Reactivate`**.

Procedure 1.3. Deleting Users

User accounts can be deleted by administrators. Deleted accounts cannot be used to log in to the RHN Satellite Server interface, or schedule actions. Deleted accounts cannot be reactivated.

Administrator accounts can only be deleted once the administrator role has been removed from the account.

Warning

Deleting accounts is irreversible; perform this action carefully. Consider deactivating the user account before deleting, in order to assess the effect deletion could have on RHN Satellite Server infrastructure.

To delete a user account:

1. Select the user's name from the list in the **Users** tab, to display the **User Details** page.
2. Check to see if the user is a Satellite administrator.

   If the user is a Satellite administrator, uncheck the box next to that role, and click **Submit**.

   If the user is not a Satellite administrator, continue to the next step.
3. Click **Delete User**.

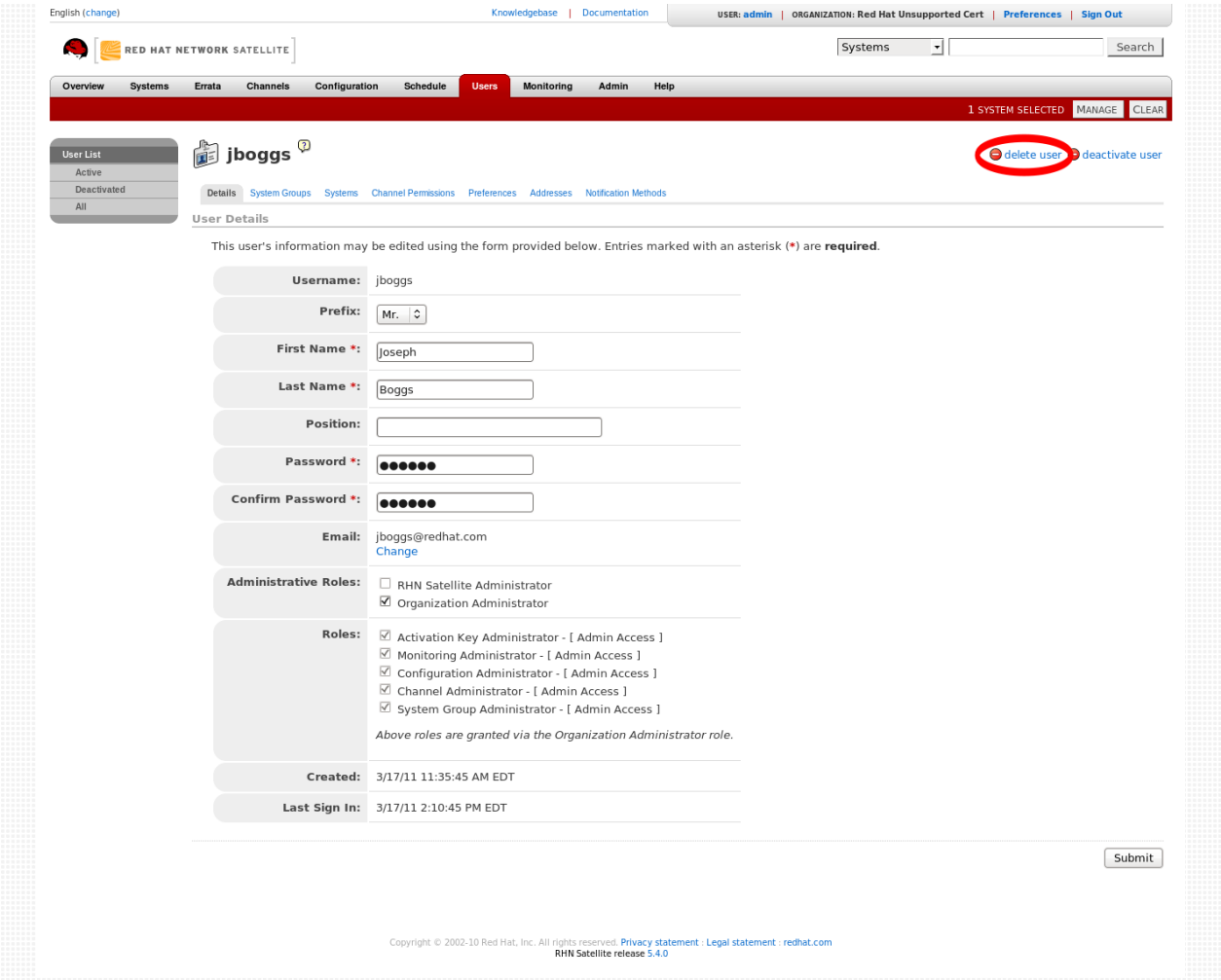
English (change)
Knowledgebase | Documentation
USER: admin | ORGANIZATION: Red Hat Unsupported Cert | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Monitoring Admin Help
1 SYSTEM SELECTED MANAGE CLEAR
User List
Active
Deactivated
All
jboggs
delete user
deactivate user
Details System Groups Systems Channel Permissions Preferences Addresses Notification Methods
User Details
This user's information may be edited using the form provided below. Entries marked with an asterisk (*) are required.
Username: jboggs
Prefix: Mr.
First Name *: Joseph
Last Name *: Boggs
Position:
Password *:
Confirm Password *:
Email: jboggs@redhat.com
Change
Administrative Roles:
RHN Satellite Administrator
Organization Administrator
Roles:
Activation Key Administrator - [Admin Access]
Monitoring Administrator - [Admin Access]
Configuration Administrator - [Admin Access]
Channel Administrator - [Admin Access]
System Group Administrator - [Admin Access]
Above roles are granted via the Organization Administrator role.
Created: 3/17/11 11:35:45 AM EDT
Last Sign In: 3/17/11 2:10:45 PM EDT
Submit
Copyright © 2002-10 Red Hat, Inc. All rights reserved. Privacy statement · Legal statement · redhat.com
RHN Satellite release 5.4.0

Figure 1.3. Deleting users

You will be asked to confirm this action, by clicking it again. Check the details, and then click **Delete User** again to confirm.

4. Once the account has been successfully deleted, the user's name will not appear in the **Active Users** list. This step is not reversible.

1.2. User Management

User accounts can be managed through the **Users** tab at the top of the RHN Satellite Server navigation bar. To change permissions and set options for a user, select their name from the displayed list to display the **User Details** page, and navigate to the appropriate tabs to make your changes. Modify account details by making the changes and clicking **Submit**.

User Roles

User roles are used to delegate responsibilities to user accounts. Each user role has a different level of responsibility and access.

To assign a user a new role, select the appropriate checkbox on the **User Details** page. Modify roles by making the changes and clicking **Submit**.

The user roles to choose from are

RHN Satellite Administrator

A special role for Satellite administrative tasks such as creating organizations, managing subscriptions, and configuring global RHN Satellite Server settings.

This role cannot be assigned on the **User Details** page. A user that already has the RHN Satellite Server administrator role can assign the role to another user by going to **Admin** → **Users**.

Organization Administrator

Performs management functions such as managing users, systems, and channels within the context of their organization. Organization administrators are automatically granted administration access to all other roles, which are signified as grayed-out checkboxes.

Activation Key Administrator

Performs activation key functions for such as creating, modifying, and deleting keys within the account.

Channel Administrator

Provides complete access to the software channels and related associations within the organization. Performs functions such as making channels globally subscribable, and creating new channels, and managing the packages within channels.

Configuration Administrator

Has complete access to the configuration channels and related associates within the organization. Performs channel and file management configuration functions in the organization.

Monitoring Administrator

Performs scheduling of probes and oversight of other monitoring infrastructure. This role is available only on RHN Satellite Servers with monitoring enabled.

System Group Administrator

This role has complete authority over the systems and system groups to which it is granted

access. Performs administrative functions such as creating new system groups, deleting assigned system groups, adding systems to groups, and managing user access to groups.

Satellite administrators can remove Satellite administrator rights from another user account, but cannot remove Satellite administrator rights from the sole remaining Satellite administrator. There must always be at least one Satellite administrator at any given time. It is possible for a Satellite administrator to remove their own Satellite administrator privileges, as long as they are not the only remaining Satellite administrator.

Chapter 2. Automatic Synchronization

Manually synchronizing the RHN Satellite Server Server repository with Red Hat Network can be an arduous task. Synchronization can be automated so that it occurs in non-peak times, such as the late evening or early morning to better balance load and ensure faster synchronization. Synchronization should occur randomly for best performance. The most effective way to automate synchronization is using **cron**.

Procedure 2.1. Automating Synchronization

1. Switch to the root user, and open the **crontab** in a text editor:

```
crontab -e
```

Note

The **crontab** will open in vi by default. To change this behavior, change the **EDITOR** variable to the name of the text editor you prefer.

2. In the **crontab**, use the first five fields (minute, hour, day, month, and weekday) to schedule the synchronization. To create a random synchronization time, use the following entry:

```
0 1 * * * perl -le 'sleep rand 9000' && satellite-sync --email >/dev/null
2>1
```

This **crontab** entry will run the synchronization job randomly between 01:00 and 03:30. It will discard ***stdout*** and ***stderr*** from **cron** to prevent duplicating the messages from **satellite-sync**. Other options can be included as needed.

3. To save the **crontab**, simply exit from the text editor. The new **cron** rules will be put in to place immediately.

Chapter 3. Backup and Restore

This chapter outlines the methods to back up, verify, and restore a Satellite system.

Backups should be conducted either nightly or weekly, depending on the amount of data being stored, and how much data can potentially be lost in the case of a system outage.

It is recommended that database backups are performed during a scheduled maintenance outage for the RHN Satellite Server, as all services will become unusable for website and client connections during the backup.

3.1. Backups

Procedure 3.1. Backing up the Embedded Database

1. Stop the RHN Satellite Server server using the **stop** command:

```
rhn-satellite stop
```

2. Switch to the Oracle user, and create the backup using the **db-control** utility:

```
su - oracle
db-control backup [directory]
```

Replace ***directory*** with the absolute path to the location where you want to store your database backup. The process will take several minutes.

3. Switch back to the root user, and start the Satellite:

```
exit
rhn-satellite start
```

4. Switch to the Oracle user, and use the **examine** option of **db-control** to check the backup time stamp and to determine if there are any missing files:

```
su - oracle
db-control examine [directory]
```

You can also use the **verify** option of **db-control** to conduct a thorough review, which includes checking the md5sum of each of the files in the backup:

```
db-control verify [directory]
```

If the verification is successful, the contents of ***directory*** are safe to be used to restore the database.

Note

Users of external databases should also perform periodic backups. Consult your external database administrator for more information on supported backup procedures.

Backing up System Files

In addition to the database, a number of system files and directories should also be backed up. The files and directories that should be backed up are:

- **/etc/sysconfig/rhn/**
- **/etc/rhn/**
- **/etc/sudoers**
- **/etc/tnsnames.ora**
- **/var/www/html/pub/**
- **/var/satellite/redhat/[0-9]*/** (This is the location for any custom RPMs)
- **/root/.gnupg/**
- **/root/ssl-build/**
- **/etc/dhcpd.conf**
- **/etc/httpd/**
- **/tftpboot/**
- **/var/lib/cobbler/**
- **/var/lib/nocpulse/**
- **/var/lib/rhn/kickstarts/**
- **/var/www/cobbler/**

If possible, back up **/var/satellite/** as well. This is a duplicate of the Red Hat RPM repository, and it will save a large download when recovering from a failure. It can be regenerated with the **satellite-sync** tool. In the case of a disconnected satellite, **/var/satellite/** must be backed up in order to be able to recover from failure.

Backing up only the files and directories listed above would require reinstalling the RHN Satellite Server ISO RPMs and re-registering the satellite in order to recover from a failure. In addition, Red Hat packages would need to be resynchronized using the **satellite-sync** tool, and the **/root/ssl-build/rhn-org-httpd-ssl-key-pair-MACHINE_NAME-VER-REL.noarch.rpm** package would need to be installed. Alternatively, you could reinstall the RHN Satellite Server without re-registering it. This can be achieved by canceling or skipping the Red Hat Network registration and SSL certificate generation sections.

The most comprehensive backup method is to back up the entire machine. This method saves time in downloading and re-installing, but also requires additional storage and time to perform the backup.

3.2. Restore from Backup

Red Hat Network database control is used to restore the embedded database from a backup.

Procedure 3.2. Restoring the Embedded Database from Backup

1. Stop the RHN Satellite Server server using the **stop** command:

```
rhn-satellite stop
```

2. Switch to the Oracle user, and restore the backup using the **db-control** utility:

```
su - oracle
db-control restore [directory]
```

Replace ***directory*** with the absolute path to the location that contains the backup. This process will verify the contents of the backup before restoring the database. The process will take several minutes.

3. Switch back to the root user, and start the Satellite:

```
exit
rhn-satellite start
```

4. Regardless of whether you are backing up an external or embedded database, when the satellite is restored from a backup, the following command should be run to schedule the restoration of search indexes the next time the **rhn-search** service is started:

```
/etc/init.d/rhn-search cleanindex
```

3.3. Automated Backups

Backup tasks can be automated so that they occur in non-peak times, such as the late evening or early morning. This also ensures they are performed regularly, and are not forgotten. The most effective way to automate backups is using **cron**.

Procedure 3.3. Automating Backups

Create a new file called **backup-db.sh** containing the following script. This script will stop the satellite, perform a database backup, and restart the satellite:

```
#!/bin/bash
{
/usr/sbin/rhn-satellite stop
su - oracle -c'
d=db-backup-$(date "+%F");
mkdir -p /tmp/$d;
db-control backup /tmp/$d
';
/usr/sbin/rhn-satellite start
} &> /dev/null
```

1. Create a new file called **move-files.sh** containing the following script. This script will use **rsync** to move the backup files to a directory to be stored:

```
#!/bin/bash
rsync -avz /tmp/db-backup-$(date "+%F") [destination] &> /dev/null
```

Replace ***[destination]*** with the path to the backup directory.

Alternatively, the following script uses **scp** to achieve the same goal:

```
#!/bin/bash
scp -r /tmp/db-backup-$(date "+%F") [destination] &> /dev/null
```

2. Switch to the root user, and open the **crontab** in a text editor:

```
crontab -e
```

Note

The **crontab** will open in vi by default. To change this behavior, change the **EDITOR** variable to the name of the text editor you prefer.

3. In the **crontab**, use the first five fields (minute, hour, day, month, and weekday) to schedule the backup scripts to run:

```
0 3 * * * backup-db.sh
0 6 * * * move-files.sh
```

This **crontab** entry will run the backup at 03:00, and transfer the backup files at 06:00. Other options can be included as needed. You can also include a clean up script to remove older backup directories and prevent the backup storage from filling up.

4. To save the **crontab**, simply exit from the text editor. The new **cron** rules will be put in to place immediately.

Chapter 4. Cloning a Machine

The command **spacewalk-clone-by-date** allows RHN Satellite customers to create custom cloned Red Hat Enterprise Linux channels based on the date Errata was made available to the Red Hat Enterprise Linux system.

4.1. Features

The following features are available with **spacewalk-clone-by-date**:

- Cloning the state of the channel as it was on a specific date
- Automating the cloning by scripts and template files
- Removing or blocking packages from channels
- Resolving package dependencies within the parent and child channels
- Filtering and acting on specific errata while ignoring others. For example, acting only on security errata and ignoring bugfixes and enhancements.

Note

The command **spacewalk-clone-by-date** needs to be run as the *root user* and the **username** needs to be either an Organizational Administrator or Channel Administrator.

4.2. Command Line Options

Table 4.1. Command Line Options Available

Option	Definition
-h, --help	Shows the help file.
-c CONFIG, --config=CONFIG	Allows the user to supply a config file that has all the options specified. Any options that can be run on the command line can be specified in this config file. The config file allows users to set up a complex list of channels that they want cloned and save the exact commands for later use.
-u USERNAME, --username=USERNAME	Specify the username to use to log in to the Satellite.
-p PASSWORD, --password=PASSWORD	Specify the password for the username
-s SERVER, --server=SERVER	Server URL to use for api connections. This defaults to https://localhost/rpc/api
-l CHANNELS, --channels=CHANNELS	Specifies which channels to clone. Channel labels must be specified in original clone pairs. When specifying clone pairs, remember to separate them with spaces. Additional channels may be specified by using the --channels option more than once.
-b BLACKLIST, --blacklist=BLACKLIST	Comma separated list of package names (or regular expressions) to exclude from cloned errata (Only added packages will be considered).
-r REMOVELIST, --removelist=REMOVELIST	Comma separated list of package names (or regular expressions) to remove from destination channel (All packages are available for removal).
-d TO_DATE, --to_date=TO_DATE	Clone errata to the specified date (YYYY-MM-DD). Allows the user to clone the original packages and any specific errata released from the creation of the original channel until the specified **TO_DATE** parameter. A time-based snapshot of the channel during the specified TO_DATE can be obtained.
-y, --assumeyes	Assume yes for any prompts that come up. This is used for unattended cloning.
-m, --sample-config	Print a sample full configuration file and exit.
-k, --skip_depsolve	Skip all dependency solving (Not recommended).
-v, --validate	Run repoclosure on the set of specified repositories.
-g, --background	Clone the errata in the background. Prompt will return quicker; before cloning is finished.

-o, --security_only	Only clone security errata (and their dependencies).This command can be used in conjunction with the **--to_date** command to only clone security errata released before or on the specified date.

4.3. Example Usage

The example below clones the **rhel-i386-server-5** channel as it is on January 1st, 2012, into the channel named my-clone-RHEL-5.

```
# spacewalk-clone-by-date --username=your_username --password=your_password --
server=satellite_server_url --channels=rhel-i386-server-5 my-clone-RHEL-5 --
to_date=2012-01-01
```

The example below will only clone security errata released on or before January 1st, 2012, ignoring any kernel updates or vim-extended packages. The command will also run the cloning process in the background on the Satellite.

```
# spacewalk-clone-by-date --username=your_username --password=your_password --
server=satellite_server_url --channels=rhel-i386-server-5 my-clone-RHEL-5 --
to_date=2012-01-01 --security_only --background --blacklist=kernel,vim-extended --
assumeyes
```

Chapter 5. Monitoring

RHN Satellite Server contains many different components, many of which can be monitored. This chapter outlines ways of performing monitoring operations for different areas of the system.

Procedure 5.1. Monitoring Tablespace

1. In Oracle databases, it is important to regularly check that the tablespaces have sufficient free space. Do this by switching user to the ***Oracle*** user, and issuing the **db-control report** command:

```
su - oracle
db-control report
Tablespace    Size  Used Avail  Use%
DATA_TBS       4.8G 3.9G  996M   80%
SYSTEM         250M 116M  133M   46%
TOOLS          128M 3M    124M   2%
UNDO_TBS       1000M 61M  938M   6%
USERS          128M 64K   127M   0%
```

2. If a tablespace is becoming full, it can be extended using the **db-control extend** command with the name of the tablespace to be extended:

```
db-control extend tablespace
```

Procedure 5.2. Monitoring RHN Satellite Server Processes

- Verify that the Satellite processes are working using the **rhn-satellite status** command:

```
rhn-satellite status
```

Chapter 6. OpenSCAP

SCAP is a standardized compliance checking solution for enterprise-level Linux infrastructure. It is a line of specifications maintained by the National Institute of Standards and Technology (NIST) for maintaining system security for enterprise systems.

In RHN Satellite Server 5.5, SCAP is implemented by the **OpenSCAP** application. **OpenSCAP** is an auditing tool that utilizes the Extensible Configuration Checklist Description Format (XCCDF). XCCDF is a standard way of expressing checklist content and defines security checklists. It also combines with other specifications such as CPE, CCE, and OVAL, to create a SCAP-expressed checklist that can be processed by SCAP-validated products.

6.1. OpenSCAP Features

OpenSCAP verifies the presence of patches by using content produced by the Red Hat Security Response Team (SRT), checks system security configuration settings and examines systems for signs of compromise by using rules based on standards/specifications.

To effectively use OpenSCAP, there are two requirements:

- A tool to verify a system confirms to a standard

  RHN Satellite Server has integrated OpenSCAP as an auditing feature from version 5.5. It allows you to schedule and view compliance scans for the system through the web interface.
- SCAP content

  SCAP content can be created from scratch if you have an understanding of at least XCCDF or OVAL. Alternatively, another option exists. XCCDF content is frequently published online under open source licenses and this content may be customized to suit your needs instead.

  Note

  Red Hat supports the use of templates to evaluate your systems. However, custom content authoring of these templates is not supported.

  Some examples of these groups are:

  - The United States Government Configuration Baseline (USGCB) for RHEL5 Desktop — Official SCAP content for desktops within federal agencies that has been developed at NIST in collaboration with Red Hat, Inc. and the United States Department of Defense (DoD) using OVAL.
  - Community-provided content
    - SCAP Security Guide for RHEL6 — Active community-run content that sources from the USGCB requirements and widely-accepted policies and contains profiles for desktop, server, and ftp server.
    - OpenSCAP Content for RHEL6 — The **openscap-content** package from the Red Hat Enterprise Linux 6 Optional Channel also provides default content guidance for Red Hat Enterprise Linux 6 systems via a template.

As SCAP was made to maintain system security, the standards that are used continually change to meet the needs of the community and enterprise businesses. New specifications are governed by NIST's SCAP Release cycle in order to provide a consistent and repeatable revision workflow.

6.2. OpenSCAP in RHN Satellite

6.2.1. Prerequisites

Package Requirements

SCAP requires these packages:

- For the Server: RHN Satellite 5.5
- For the Client: **spacewalk-oscap** package (available from the RHN Tools Child Channel)

Entitlement Requirements

A Management entitlement is required for scheduling scans.

Other Requirements

For the Client: Distributing the XCCDF content to client machines

Distributing XCCDF content to client machines can be done through the following methods:

- Traditional Methods (CD, USB, nfs, scp, ftp)
- Satellite Scripts
- RPMs

  Custom RPMs are the recommended way to distribute SCAP content to other machines. RPM packages can be signed and verified to ensure their integrity. Installation, removal, and verification of RPM packages can be managed from the user interface.

6.2.2. Performing Audit Scans

OpenSCAP integration in the RHN Satellite Server gives the ability to perform audit scans on client systems. This section discusses the two methods available.

Procedure 6.1. Scans via the Web Interface

To perform a scan through the Satellite Web Interface:

1. Log in to the Satellite web interface.
2. Click on **Systems** → **Target System**.
3. Click on **Audit** → **Schedule**
4. Fill in the ***Schedule New XCCDF Scan*** form:
   - Command-line Arguments: Additional arguments for the oscap tool can be added into this field. There are only two command line arguments that are permitted. These are:

     `--profile PROFILE` — Selects a particular profile from the XCCDF document. Profiles are determined by the XCCDF xml file and can be checked using the ***`Profile id`*** tag. For example:

     ```
     Profile id="RHEL6-Default"
     ```

     Note

     Certain versions of OpenSCAP need the --profile command-line argument or the scan will fail.

--skip-valid — Do not validate input/output files. Users without a well-formed XCCDF content may choose to use this to bypass the file validation process.

If no command-line argument is passed, it will use the default profile.

- Path to XCCDF Document: This is a required field. The ***path*** parameter points to the content location on the client system. For example: **/usr/local/scap/dist_rhel6_scap-rhel6-oval.xml**

Warning

The xccdf content is validated before it is run on the remote system. Specifying invalid arguments can make spacewalk-oscap fail to validate or run. Due to security concerns the 'osccap xccdf eval' command only accepts a limited set of parameters.

5. Run the **rhn_check** to ensure that the action is being picked up by the client system.

```
rhn_check -vv
```

Note

Alternatively, if **rhnsd** or **osad** are running on the client system, the action will be picked up by these services. To check if they are running:

```
service rhnsd start
```

or

```
service osad start
```

To view the results of the scan, please refer to Section 6.2.3, “How to View SCAP Results”.

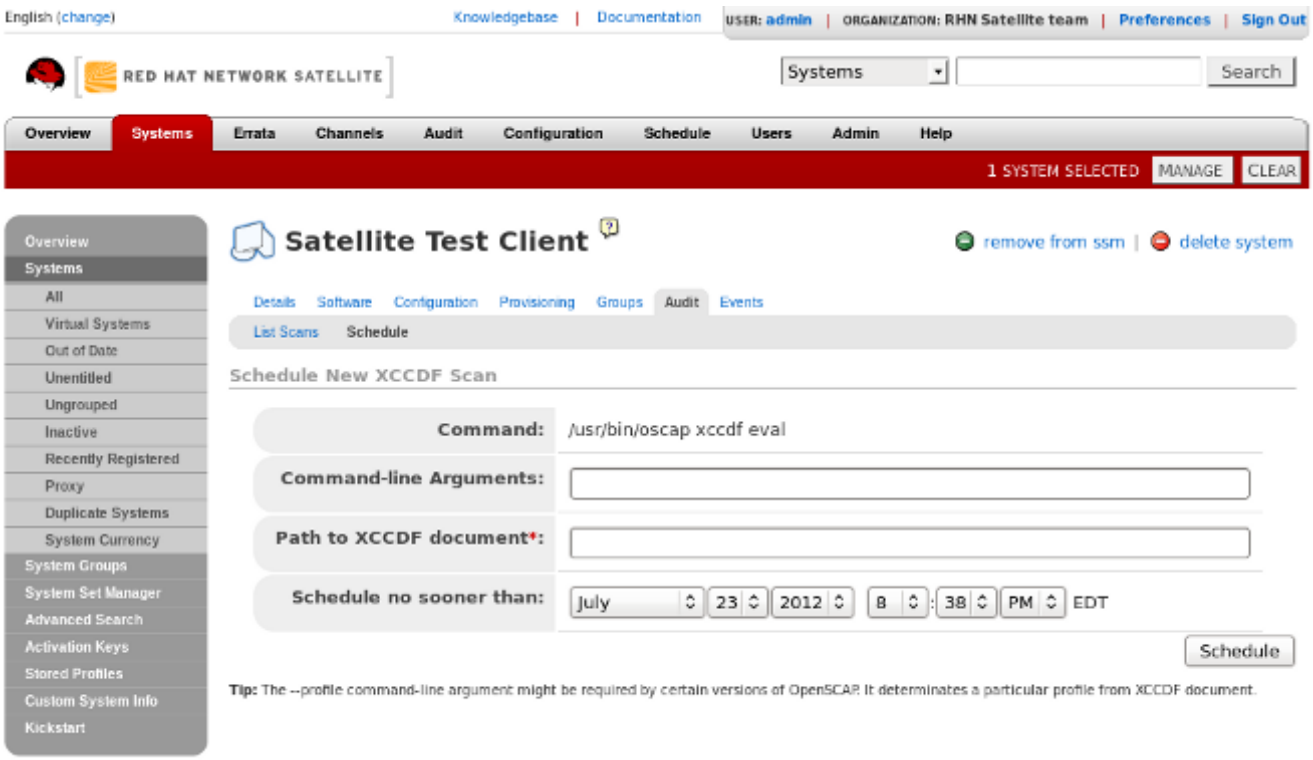

Figure 6.1. Scheduling a Scan via Web UI

Procedure 6.2. Scans via API

To perform an audit scan via API:

1. Choose an existing script or create a script for scheduling a system scan through **`system.scap.scheduleXccdfScan`**, the front end API.

   Example Script:

   ```
   #!/usr/bin/python
   client = xmlrpclib.Server('https://spacewalk.example.com/rpc/api')
   key = client.auth.login('username', 'password')
   client.system.scap.scheduleXccdfScan(key, 1000010001,
       '/usr/local/share/scap/usgcb-rhel5desktop-xccdf.xml',
       '--profile united_states_government_configuration_baseline')
   ```

   Where:

   - 1000010001 is the ***`system ID (sid)`***.
   - **`/usr/local/share/scap/usgcb-rhel5desktop-xccdf.xml`** is the path parameter that points to the content location on the client system. In this case, it assumes USGSB content in the **`/usr/local/share/scap`** directory.
   - **`--profile united_states_government_configuration_baseline`** represents the additional argument for the oscap tool. In this case, it is using the USCFGB.
2. Run the script on the command-line interface of any system. The system needs the appropriate python and xmlrpc libraries installed.
3. Run the **`rhn_check`** to ensure that the action is being picked up by the client system.

   ```
   rhn_check -vv
   ```

Note

Alternatively, if **rhnsd** or **osad** are running on the client system, the action will be picked up by these services. To check if they are running:

```
service rhnsd start
```

or

```
service osad start
```

6.2.3. How to View SCAP Results

There are three methods of viewing the results of finished scans:

- Via the web interface. Once the action has been executed, the results should show up on the system's **Audit** Tab. This page is discussed in Section 6.2.4, “OpenSCAP Satellite Pages”.
- Via the API functions in handler **system.scap**.
- Via the Satellite's **spacewalk-reports** tool by running these commands:

```
# /usr/bin/spacewalk-reports system-history-scap
# /usr/bin/spacewalk-reports scap-scan
# /usr/bin/spacewalk-reports scap-scan-results
```

6.2.4. OpenSCAP Satellite Pages

The following sections describe the tabs in the RHN Satellite Web UI that encompasses OpenSCAP.

6.2.4.1. Audit

The **Audit** tab on the top navigation bar is the encompassing page for the OpenSCAP functionality in RHN Satellite Server 5.5. Clicking on this tab will enable you to view completed OpenSCAP scans, search, and compare them.

Audit → All Scans

All Scans is the default page that appears when the **Audit** tab is chosen. This page displays all completed OpenSCAP scans which the viewer has permission to see. Permissions for scans derive from system permissions.

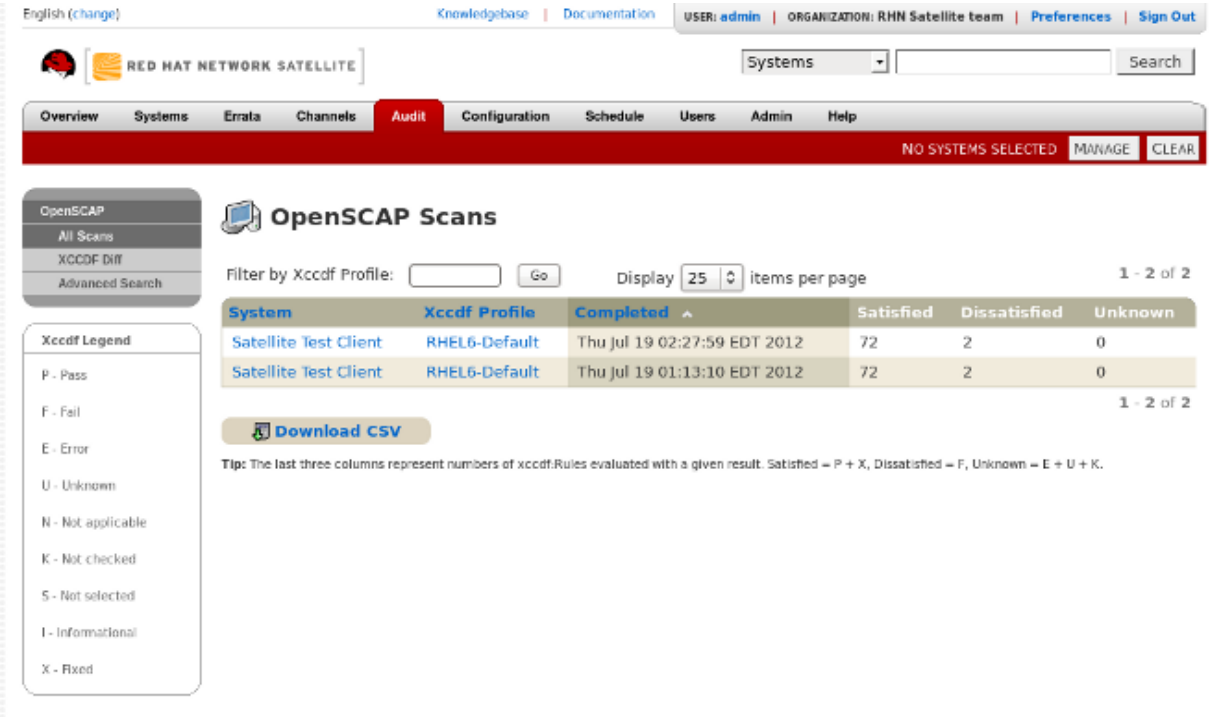

Figure 6.2. Audit ⇒ All Scans

For each scan, the following information is displayed:

System
: the scan's targeted system

XCCDF Profile
: the evaluated profile

Completed
: time of completion

Satisfied
: number of rules satisfied/passed. A rule is considered to be satisfied if the result is the evaluation is either Pass or Fixed.

Dissatisfied
: number of rules dissatisfied/failed. A rule is considered to be dissatisfied if the result of the evaluation is a Fail.

Unknown
: number of rules which failed to evaluate. A rule is considered to be Unknown if the result of the evaluation is an Error, Unknown or Not Checked.

The evaluation of XCCDF rules may also return statuses like **`Informational`**, **`Not`**

Applicable, or **not Selected**. In such cases, the given rule is not included in the statistics on this page. See **System Details → Audit** for information on those.

Audit → XCCDF Diff

XCCDF Diff is an application which visualizes the comparison of two XCCDF scans. It shows metadata for two scans as well as the lists of results.

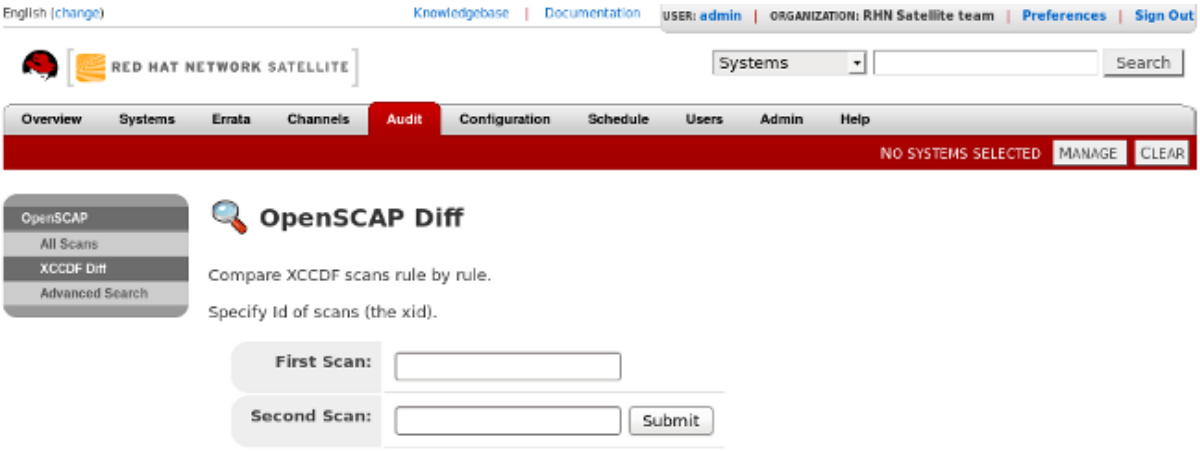

Figure 6.3. Audit ⇒ XCCDF Diff

You can access the **diff** of similar scans directly by clicking on icon at the **List Scans** page or you can **diff** arbitrary scans by specifying their id.

Items that show up in only one of the compared scans are considered to be "varying". Varying items are always highlighted in beige. There are three possible comparison modes: **Full Comparison** which shows all the scan items, **Only Changed Items** which shows items that have changed, and finally **Only Invariant Items** which shows unchanged or similar items.

Audit → Advanced Search

The Search page allows you to search through your scans according to specified criteria, including:

- rule results
- targeted machine
- time frame of the scan

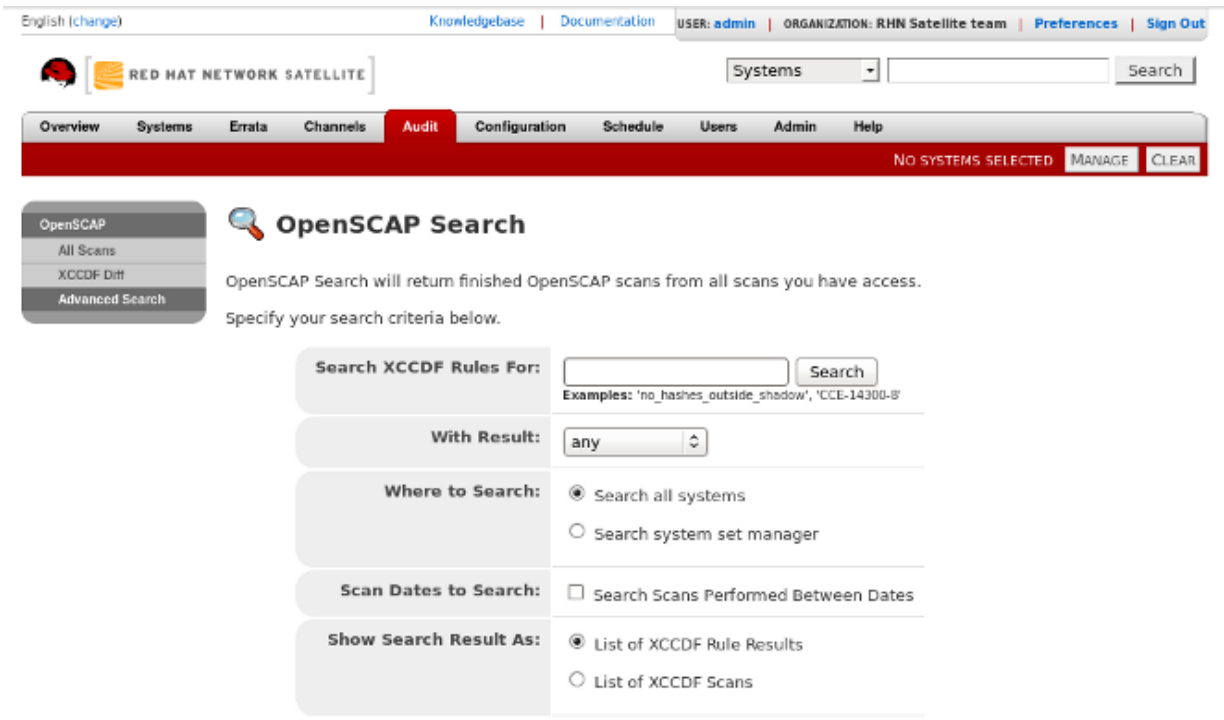

Figure 6.4. Audit ⇒ Advanced Search

The search either returns a list of results or list of scans which are included in the results.

6.2.4.2. Systems → System Details → Audit

This tab and its subtabs allow you to schedule and view compliance scans for the system. A scan is performed by the SCAP tool, which implements NIST's standard SCAP (Security Content Automation Protocol). To scan the system, make sure that the SCAP content is prepared and all prerequisites in Section 6.2.1, “Prerequisites” are met.

Systems → System Details → Audit → List Scans

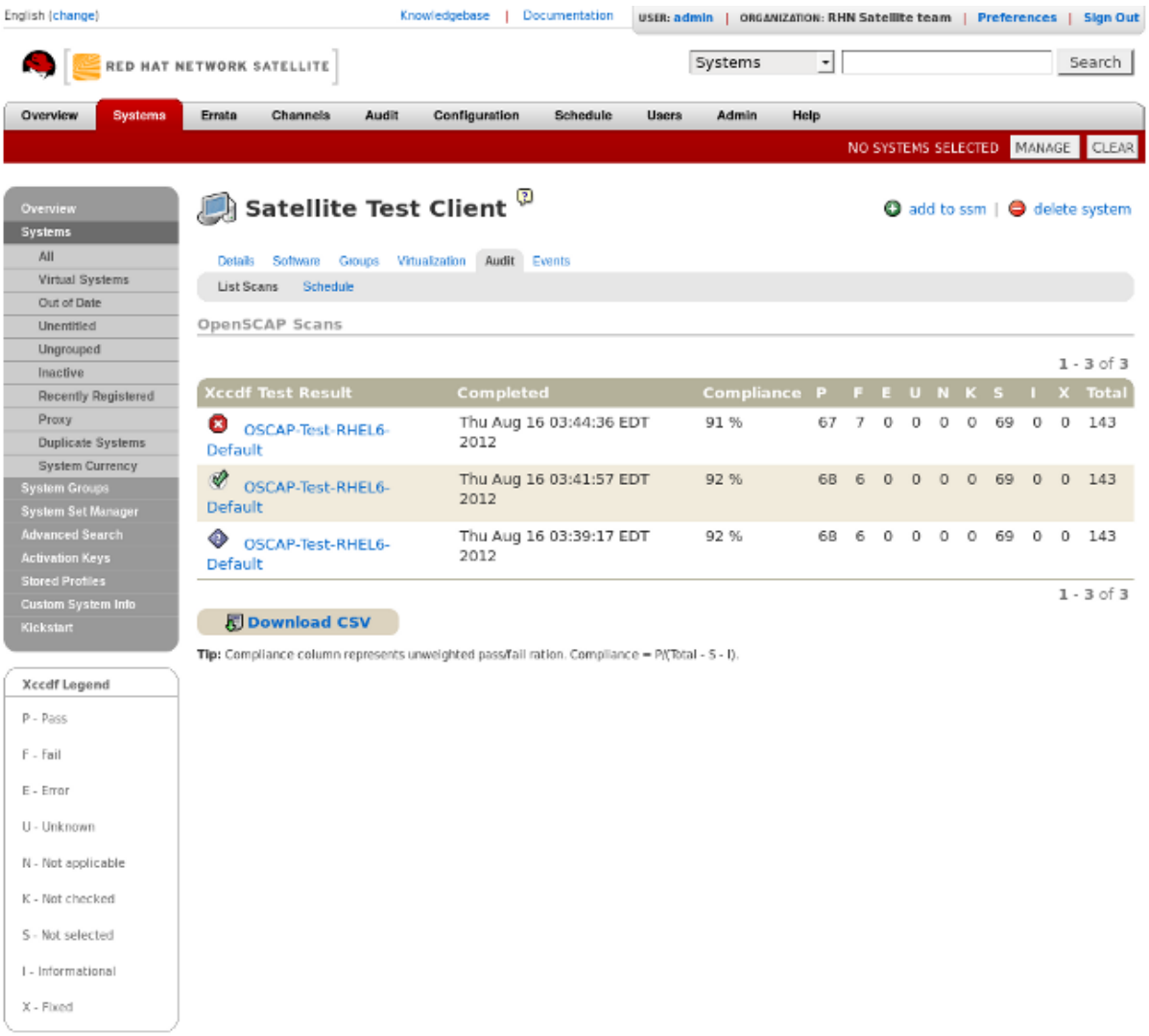

Figure 6.5. Systems ⇒ System Details ⇒ Audit ⇒ List Scans Scan Results

This subtab lists a summary of all scans completed on the system. The columns are as follows:

Table 6.1. OpenSCAP Scan Labels

Column Label	Definition
XCCDF Test Result	The scanned test result name which provides a link to the detailed results of the scan.
Completed	The exact time the scan finished
Compliance	The unweighted pass/fail ratio of compliance based on the Standard used
P	Number of Checks that Passed
F	Number of Checks that Failed
E	Errors experienced in the Scan
U	Unknown
N	Not applicable to the machine
K	Not checked
S	Not Selected
I	Informational
X	Fixed
Total	Total number of checks

Each line starts with an icon indicating the results of a comparison to a previous similar scan. The icons indicate that in the newer scan there is either:

- — no difference compared to the previous scan
- — arbitrary differences
- — major differences, either there are more failures than the previous scan or less passes
- — no comparable scan was found, therefore, no comparison was made.

Systems → System Details → Audit → Scan Details

This page contains the results of a single scanning. It can be divided into two parts:

- Details of the XCCDF Scan

  The details of the scan gives you:
  - the general information of the file path
  - what command-line arguments were used
  - who scheduled it
  - what is the benchmark identifier and version
  - the Profile Identifier
  - the Profile Title
  - when it was started and completed
  - any error output.
- XCCDF Rule Results

  The rule results provide the full list of XCCDF rule identifiers, identifying tags and the result

for each of these rule results. This list can be filtered by a specific result.

Systems → System Details → Audit → Schedule

This subtab is where new scans can be scheduled. Additional command line arguments can be provided, along with the path to the XCCDF document on the system which is being scanned. Based on the "**Schedule no sooner than**" parameter, the scan will be performed at the system's next scheduled check-in with the Satellite Server. For more information about how to schedule via the Satellite web interface, refer to Procedure 6.1, “Scans via the Web Interface” in this chapter.

Chapter 7. PAM Authentication

RHN Satellite Server supports network-based authentication systems using Pluggable Authentication Modules (PAM). PAM is a suite of libraries that helps system administrators integrate the RHN Satellite Server with a centralized authentication mechanism, which eliminates the need to remember multiple passwords.

RHN Satellite Server is able to use PAM with LDAP, Kerberos, Directory Server, or another network-based authentication system. This chapter outlines setting up PAM to work with your organization's authentication infrastructure.

Procedure 7.1. Setting up PAM authentication

1. Ensure you have the latest version of the **`selinux-policy-targeted`** package:

```
# yum update selinux-policy-targeted
```

2. Set the **`allow_httpd_mod_auth_pam`** SELinux boolean to on:

```
# setsebool -P allow_httpd_mod_auth_pam 1
```

3. Open the **`/etc/rhn/rhn.conf`** file in your preferred text editor, and add the following line. This will create a PAM service file at **`/etc/pam.d/rhn-satellite`**:

```
pam_auth_service = rhn-satellite
```

4. To set up authentication, open the **`/etc/pam.d/rhn-satellite`** service file in your preferred text editor, and add the appropriate rules. For more detail about configuring PAM, refer to the *Pluggable Authentication Modules (PAM)* in the *Red Hat Enterprise Linux Deployment Guide*.

Note

Check that the PAM authentication works correctly before using it with RHN Satellite Server.

Example 7.1. Using PAM with Kerberos on a Red Hat Enterprise Linux 5 i386 system

This example enables PAM with Kerberos authentication on a Red Hat Enterprise Linux 5 i386 system.

Open the **`/etc/pam.d/rhn-satellite`** service file in your preferred text editor, and add the following rules:

```
#%PAM-1.0
auth        required      pam_env.so
auth        sufficient    pam_krb5.so no_user_check
auth        required      pam_deny.so
account     required      pam_krb5.so no_user_check
```

For Kerberos-authenticating users, change the password by using **`kpasswd`**. Do not change the password on the RHN website as this method will only change the local password on the Satellite server. Local passwords are not in use if PAM is enabled for that user.

Example 7.2. Using PAM with LDAP

This example enables PAM with LDAP authentication.

Open the **/etc/pam.d/rhn-satellite** service file in your preferred text editor, and add the following rules:

```
#%PAM-1.0
auth          required      pam_env.so
auth          sufficient    pam_ldap.so no_user_check
auth          required      pam_deny.so
account       required      pam_ldap.so no_user_check
```

Chapter 8. RPMs

As part of automated installations, administrators will often deploy custom applications not provided by Red Hat, such as backup and monitoring software. In order to do this, this software must be packaged as an RPM. An RPM build environment can be set up on a system running Red Hat Enterprise Linux. It should be noted that the build system must contain the same version of packages which are used in target systems. This means that a Red Hat Enterprise Linux 5 system must be used to build RPMs for Red Hat Enterprise Linux 5 based systems and a Red Hat Enterprise Linux 6 system for Red Hat Enterprise Linux 6 RPMs.

The **rpm-build** package must be installed on the build system as a minimum requirement. Additional packages such as compilers and libraries may also be needed.

Production-ready RPM packages should be signed with a GPG key, which allows users to verify the origin and integrity of packages. The passphrase of the GPG key used for signing RPMs should be known only to a trusted group of administrators.

Procedure 8.1. Creating a GPG Key

Important

The following commands will initiate GPG key creation and export it in a format suitable for distributing to client systems. The created key should be stored safely and backed up.

1. Make a directory for creating the key:

```
mkdir -p ~/.gnupg
```

2. Generate the key pair:

```
gpg --gen-key
```

You will need to select the kind of key, the keysize, and how long the key should be valid for (press **enter** to accept the default values). You will also need to specify a name, comment, and email address:

```
Real name: rpmbuild
Email address: rpmbuild@example.com
Comment: this is a comment
You selected this USER-ID:
    "rpmbuild (this is a comment) <rpmbuild@example.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
```

Press **O** to accept the details and continue.

3. List all keys with their fingerprints:

```
gpg --list-keys --fingerprint
```

4. Export the keys:

```
gpg --export --armor "rpmbuild <rpmbuild@example.com>" > EXAMPLE-RPM-GPG-
KEY
```

5. Import the key to the RPM database to allow RPM origin and integrity verification by running the **gpg --import** as root on all target systems:

```
rpm --import EXAMPLE-RPM-GPG-KEY
```

   This will occur automatically during client installations, and should not need to be run manually.

6. Once an RPM has been created it can be signed with the GPG key and uploaded to the correct channel:

```
rpm --resign package.rpm
rhnpush --server=http[s]://satellite.server/APP package.rpm --
channel=custom-channel-name
```

7. To verify an RPM package, navigate to the directory that contains the package, and run the following commands:

```
rpm –qip package.rpm
rpm -K package.rpm
```

Procedure 8.2. Building RPMs

1. Create a non-privileged user account called **rpmbuild** for building packages. This will allow several administrators to share the build environment and the GPG key.
2. In the home directory for the **rpmbuild** user, **/home/rpmbuild**, create a file called **.rpmmacros**:

```
touch /home/rpmbuild/.rpmmacros
```

3. Open the **.rpmmacros** file in your preferred text editor, and add the following lines. The *_gpg_name* must match the name for the GPG key used for signing RPMs:

```
%_topdir            %(echo $HOME)/rpmbuild
%_signature         %gpg
%_gpg_name          rpmbuild <rpmbuild@example.com>
```

   The directory listing for the defined top level directory (**/home/rpmbuild/rpmbuild** in the example above) must have the same directory layout that is present under **/usr/src/redhat**.

Example 8.1. RPM Specification File

The following is a basic example of an RPM spec file. When building, it should be located in the **SPECS** directory under the **_topdir** as defined in user's **.rpmmacros** file. The corresponding source and patch files should be located in the **SOURCES** directory.

```
Name: foo
Summary: The foo package does foo
Version: 1.0
Release: 1
License: GPL
Group: Applications/Internet
URL: http://www.example.org/
Source0 : foo-1.0.tar.gz
Buildroot: %{_tmppath}/%{name}-%{version}-%{release}-root
Requires: pam
BuildPrereq: coreutils
%description
This package performs the foo operation.
%prep
%setup -q
%build
%install
mkdir -p %{buildroot}/%{_datadir}/%{name}
cp -p foo.spec %{buildroot}/%{_datadir}/%{name}
%clean
rm -fr %{buildroot}
%pre
# Add user/group here if needed
%post
/sbin/chkconfig --add food
%preun
if [ $1 = 0 ]; then # package is being erased, not upgraded
    /sbin/service food stop > /dev/null 2>&1
    /sbin/chkconfig --del food
fi
%postun
if [ $1 = 0 ]; then # package is being erased
    # Any needed actions here on uninstalls
else
    # Upgrade
    /sbin/service food condrestart > /dev/null 2>&1
fi
%files
%defattr(-,root,root)
%{_datadir}/%{name}
%changelog
* Mon Jun 16 2003 Some One <one@example.com>
- fixed the broken frobber (#86434)
```

Chapter 9. Boot Devices

Automated installation (or *kickstart*) is an essential part of efficient system provisioning. This chapter describes how to prepare different types of boot media for use with kickstarting clients.

For more detailed information on using kickstart for provisioning, see the *RHN Satellite Server Getting Started Guide*.

The Red Hat Enterprise Linux CD boot image **boot.iso** is a required prerequisite for creating boot devices. Make sure that this is available somewhere on the system and take note of its location.

Procedure 9.1. CD Boot Media

Note

The backslash "****" is used below to represent a continuation of one line at the shell prompt.

1. Create a working directory for the boot image:

```
mkdir -p temp cd/isolinux
```

2. Mount the boot image to the **temp** directory:

```
mount -o loop boot.iso temp
```

3. Copy the required files for a CD Boot Media device to the previously created directory:

```
cp -aP temp/isolinux/* cd/isolinux/
```

4. Unmount the **temp** directory and change the permissions on the **cd** directory to be readable and writable to the user:

```
umount temp
chmod -R u+rw cd
```

5. Change to the **./cd** directory:

```
cd ./cd
```

6. Copy the **/usr/lib/syslinux/menu.c32** file to the CD:

```
cp -p /usr/lib/syslinux/menu.c32 isolinux
```

7. Open the **isolinux/isolinux.cfg** file in your preferred text editor, and add the following line:

```
mkisofs -o ./custom-boot.iso -b isolinux/isolinux.bin -c isolinux/boot.cat -
no-emul-boot \
  -boot-load-size 4 -boot-info-table -J -l -r -T -v -V "Custom RHEL Boot" .
```

8. Customize any boot parameters and targets in **isolinux.cfg** as needed for CD booting.
9. Burn the details to the CD to complete the procedure.

Procedure 9.2. PXE Boot

1. Create a working directory for the boot image:

```
mkdir -p temp pxe/pxelinux.cfg
```

2. Mount the boot image to the **temp** directory:

```
mount -o loop boot.iso temp
```

3. Copy the required files for a PXE Boot device to the previously created directory:

```
cp -aP temp/isolinux/* pxe/
```

4. Unmount the **temp** directory and change the permissions on the **cd** directory to be readable and writable to the user:

```
umount temp
chmod -R u+rw pxe
```

5. Change to the **/pxe** directory:

```
cd ./pxe
```

6. Copy the **/usr/lib/syslinux/menu.c32** file to the **/pxe** directory:

```
cp -p /usr/lib/syslinux/menu.c32 .
```

7. Move the **isolinux.cfg** file to **pxelinux.cfg/default**:

```
mv isolinux.cfg pxelinux.cfg/default
```

8. Remove the temporary files:

```
rm -f isolinux.bin TRANS.TBL
```

9. Copy the **/usr/lib/syslinux/pxelinux.0** file to the **/pxe** directory:

```
cp -p /usr/lib/syslinux/pxelinux.0 .
```

10. Open the **pxelinux.cfg/default** file in your preferred text editor, and customize any boot parameters and targets as needed for PXE booting.

Procedure 9.3. USB Boot Media

Warning

Be extremely careful when carrying out these command as root (required for most critical parts). These commands access device files and using them incorrectly could irrecoverably damage your system. The example below uses **/dev/loop0** for mounting, make sure you use the correct device for your system. You can check which is the correct device using the **losetup -f** command.

1. Create a working directory for the boot image:

```
mkdir -p temp usb/extlinux
```

2. Mount the boot image to the **temp** directory:

```
mount -o loop boot.iso temp
```

3. Copy the required files for a USB Media Boot device to the previously created directory:

```
cp -aP temp/isolinux/* usb/extlinux/
```

4. Unmount the **temp** directory and change the permissions on the **cd** directory to be readable and writable to the user:

```
umount temp
chmod -R u+rw usb
```

5. Change to the **/usb** directory:

```
cd ./usb
```

6. Copy the **/usr/lib/syslinux/menu.c32** file to the **extlinux/** directory:

```
cp -p /usr/lib/syslinux/menu.c32 extlinux/
```

7. Move the **extlinux/isolinux.cfg** file to **extlinux/extlinux.conf**:

```
mv extlinux/isolinux.cfg extlinux/extlinux.conf
```

8. Remove the temporary files:

```
rm -f extlinux/isolinux.bin extlinux/TRANS.TBL
```

9. Convert the **custom-boot.img** file and copy it:

```
dd if=/dev/zero of=./custom-boot.img bs=1024 count=30000
```

10. Discover the correct mounting location for the loopback device:

```
losetup -f
/dev/loop0
```

Set up the loopback device with the boot image:

```
losetup /dev/loop0 ./custom-boot.img
```

11. Open the **fdisk** utility:

```
fdisk /dev/loop0
```

Create one primary bootable partition on the device. This can be done by using the following key press combination: **n p 1 Enter Enter a 1 p w**

12. Copy the master boot record (MBR) to the loopback device:

```
dd if=/usr/lib/syslinux/mbr.bin of=/dev/loop0
```

13. Add partition maps to the loopback device:

```
kpartx -av /dev/loop0
```

14. Create the file system:

```
mkfs.ext2 -m 0 -L "Custom RHEL Boot" /dev/mapper/loop0p1
```

15. Mount the device:

```
mount /dev/mapper/loop0p1 temp
```

16. Delete temporary files:

```
rm -rf temp/lost+found
```

17. Copy the **extlinux/** directory to a temporary location:

```
cp -a extlinux/* temp/
```

18. Install the bootloader in the temporary location:

```
extlinux temp
```

19. Unmount the temporary location:

```
umount temp
```

20. Delete the partition maps on the loopback device:

```
kpartx -dv /dev/loop0
```

21. Delete the loopback device:

```
losetup -d /dev/loop0
```

    Synchronize the file system changes:

```
sync
```

22. Open the **extlinux.conf** file in your preferred text editor, and customize any boot parameters and targets as needed for USB booting.
23. Transfer the image to a USB device to complete the procedure. Insert the device, and run the **dmesg** command to check the mounting location. In this example, it is **/dev/sdb**.

    Unmount the USB device:

```
umount /dev/sdb
```

    Copy the image to the USB device:

```
dd if=./custom-boot.img of=/dev/sdb
```

Chapter 10. Organizations

RHN Satellite enables administrators to divide their deployments into organized containers. These containers (or *organizations*) assist in maintaining clear separation of purpose and ownership of systems and the content deployed to those systems.

RHN Satellite supports the creation and management of multiple *organizations* within one installation, allowing for the division of systems, content, and subscriptions across different groups. This chapter summarizes the basic concepts and tasks for multiple organization creation and management.

The **Organizations** Web interface allows administrators to view, create, and manage multiple Satellite organizations. Satellite administrators can allocate software and system entitlements across various organizations, as well as control an organization's access to system management tasks.

Satellite Administrators can create new organizations and assign administrators and entitlements for those organizations. Organization Administrators can assign groups, systems, and users for their organization. This division allows organizations to perform administrative tasks on their own without affecting other organizations.

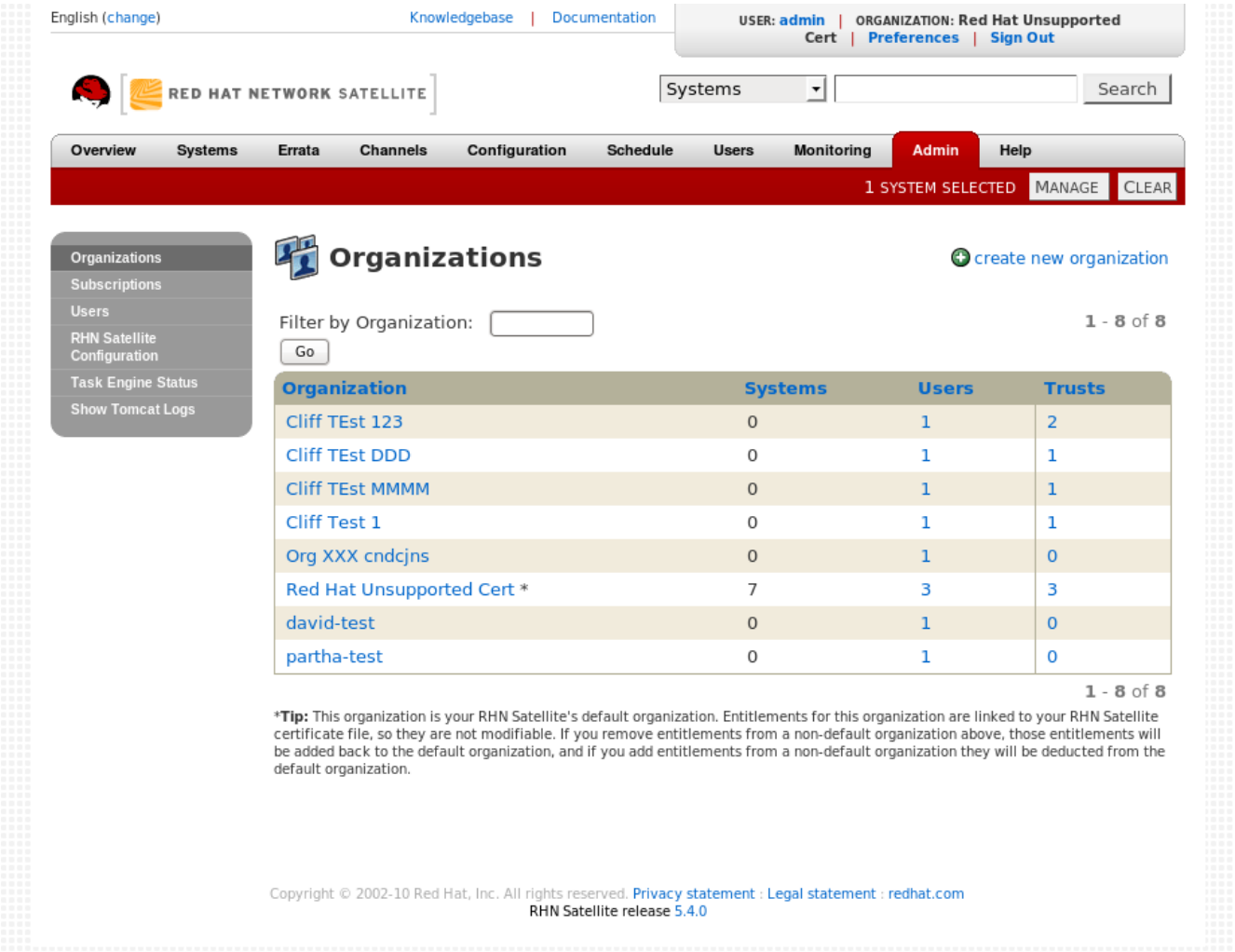
English (change)
Knowledgebase | Documentation
USER: admin | ORGANIZATION: Red Hat Unsupported Cert | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Monitoring Admin Help
1 SYSTEM SELECTED MANAGE CLEAR
Organizations
Subscriptions
Users
RHN Satellite Configuration
Task Engine Status
Show Tomcat Logs
Organizations
create new organization
Filter by Organization:
Go
1 - 8 of 8
Organization Systems Users Trusts
Cliff TEst 123 0 1 2
Cliff TEst DDD 0 1 1
Cliff TEst MMMM 0 1 1
Cliff Test 1 0 1 1
Org XXX cndcjns 0 1 0
Red Hat Unsupported Cert * 7 3 3
david-test 0 1 0
partha-test 0 1 0
1 - 8 of 8
*Tip: This organization is your RHN Satellite's default organization. Entitlements for this organization are linked to your RHN Satellite certificate file, so they are not modifiable. If you remove entitlements from a non-default organization above, those entitlements will be added back to the default organization, and if you add entitlements from a non-default organization they will be deducted from the default organization.
Copyright © 2002-10 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
RHN Satellite release 5.4.0

Figure 10.1. Admin

The **Organizations** page contains a listing of organizations across the Satellite, with both User and System counts assigned to each organization. The **Organizations** page also features a **Trusts** page for any organizational trusts established.

10.1. Creating Organizations

Procedure 10.1. Creating an Organization

1. To create a new organization, open the **Admin** menu, and select **Organizations** => **Create New Organization**.

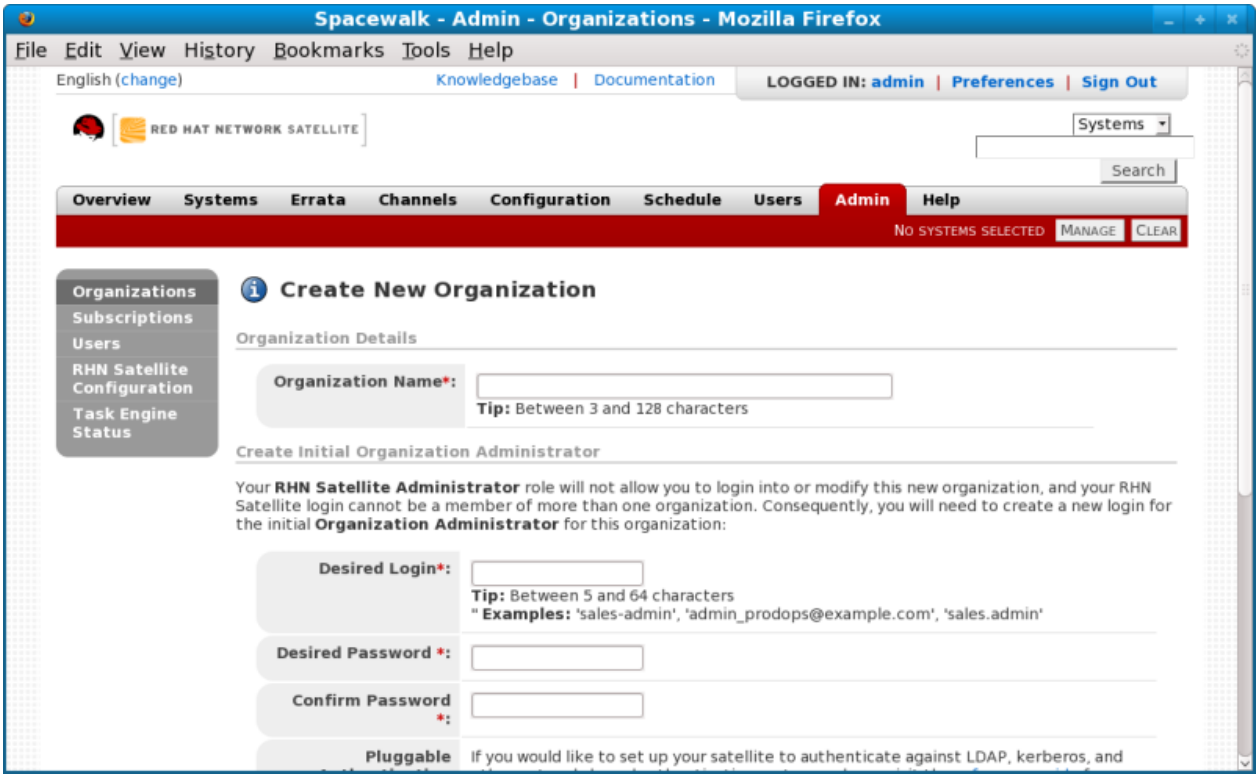
Spacewalk - Admin - Organizations - Mozilla Firefox
File Edit View History Bookmarks Tools Help
English (change)
Knowledgebase | Documentation
LOGGED IN: admin | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Admin Help
NO SYSTEMS SELECTED MANAGE CLEAR
Organizations
Subscriptions
Users
RHN Satellite Configuration
Task Engine Status
Create New Organization
Organization Details
Organization Name*:
Tip: Between 3 and 128 characters
Create Initial Organization Administrator
Your RHN Satellite Administrator role will not allow you to login into or modify this new organization, and your RHN Satellite login cannot be a member of more than one organization. Consequently, you will need to create a new login for the initial Organization Administrator for this organization:
Desired Login*:
Tip: Between 5 and 64 characters
" Examples: 'sales-admin', 'admin_prodops@example.com', 'sales.admin'
Desired Password *:
Confirm Password *:
Pluggable
If you would like to set up your satellite to authenticate against LDAP, kerberos, and

Figure 10.2. Create New Organization

2. Type the organization name into the appropriate text box. The name should be between 3 and 128 characters.
3. Create an administrator for the organization, by providing the following information:
   - Enter a **`Desired Login`** for the organization administrator, which should be between 3 and 128 characters long. Consider creating a descriptive login name for the Organization Administrator account that matches administrative login names with the organization.
   - Create a **`Desired Password`** and **`Confirm`** the password.
   - Type in the **`Email`** address for the organization administrator.
   - Enter the **`First Name`** and **`Last Name`** of the organization administrator.
4. Click the **`Create Organization`** button to complete the process.

Once the new organization is created, the **`Organizations`** page will display with the new organization listed.

Satellite Administrators should consider reserving the ***`organization 1`*** Organization Administrator account for themselves. This will give them the ability to log in to the organization if required.

Important

If RHN Satellite is configured for PAM authentication, avoid using PAM accounts for the one Satellite administrative organization administrator account in new organizations. Instead, create a Satellite-local account for organization administrators and reserve PAM-authenticated accounts for Satellite logins with less elevated privileges. This will discourage users from logging in to the RHN Satellite with elevated privileges, as the potential for making mistakes is higher using these accounts.

10.2. Managing Entitlements

Once you have created a new organization, it is important to assign entitlements for it. You will need system entitlements, such as Management and Provisioning, for each system. You will also need channel entitlements, such as **`rhel-server`** or **`rhn-tools`**, for systems that use channels other than custom channels. Management system entitlements are a base requirement for an organization to function correctly. The number of management entitlements allocated to an organization is equivalent to the maximum number of systems that can register to that organization on the RHN Satellite, regardless of the number of software entitlements available. For example, if there are 100 Red Hat Enterprise Linux Client entitlements available in total, but only 50 management system entitlements are available to the organization, only 50 systems are able to register to that organization.

Red Hat Network Tools software channel entitlements will also need to be granted to each organization. The Red Hat Network Tools channel contains various client software required for extended RHN Satellite functionality, such as clients necessary for configuration management and kickstart support as well as the **`rhn-virtualization`** package, which is necessary for the entitlements of Xen and KVM virtual guests to be counted correctly.

To access the **`Subscriptions`** interface, open the **Admin** menu, and select **Organization**. Choose an organization from the list and select the **Subscriptions** tab.

Within the **Subscriptions** interface, open the **`Software Channel Entitlements`** tab to see all entitlements for all organizations, and their usage.

Within the **`Software Channel Entitlements`** tab, the **`Organizations`** tab allows Satellite Administrators to adjust the number of software channels available to each organization. Type in the number (within the range listed in **`Possible Values`**) and click the **`Update Organization`** button to change this value.

Channel entitlements can be either *Regular* or *Flex*. Any system can use a regular entitlement. Flex entitlements can only be used by systems that have been detected as being guests of a supported virtualization type.

Note

Organization Administrators that create a custom channel can only use that channel within their organization unless an Organizational Trust is established between the organizations that want to share the channel. For more information about organizational trusts, refer to Section 10.5, “Organizational Trusts”.

The **`Organizations`** tab also contains a **`Subscriptions`**+**`System Entitlements`** section, which

details:

- **Total**: The total number of channel entitlements for the Satellite.
- **Available**: The number of entitlements currently available for allocation.
- **Usage**: The number of entitlements currently in use by all organizations, compared to the total number of entitlements allocated.

For example, if the **Total** column is 100 and the **Available** column is 70, that means 30 entitlements are allocated for organizations. The **Usage** column shows how many of those 30 allocated entitlements are in use by organizations besides the base organization. So if the **Usage** column reads **24 of 30 (80%)**, that means 24 channel entitlements are distributed to Satellite organizations (other than ***organization 1***) out of the 30 that have been allocated.

Within the **Subscriptions** interface, select the **Software Channel Entitlements** tab to see all entitlements throughout all organizations, and their usage. Click on an organization to display the **Details** page, which provides further information about the organization.

- **Active Users**: The number of users in the organization
- **Systems**: The number of systems subscribed to the organization.
- **System Groups**: The number of groups subscribed to the organization.
- **Activation Keys**: The number of activation keys available to the organization.
- **Kickstart Profiles**: The number of kickstart profiles available to the organization.
- **Configuration Channels**: The number of Configuration Channels available to the organization.

From this page, you can delete the organization by clicking the **Delete Organization** link.

10.3. Configuring Systems in an Organization

Once an organization has been created and entitlements assigned to it, systems can then be assigned.

There are two ways to register a system against a particular organization:

Registering with username and password

If you provide a username and password created for a specified organization, the system will be registered to that organization. For example, if **user-123** is a member of the **Central IT** organization on the Satellite, the following command on any system would register that system to the **Central IT** organization on your Satellite:

```
rhnreg_ks --username=user-123 --password=foobar
```

Note

The ***--orgid*** parameters in **rhnreg_ks** are *not related* to Satellite registration or RHN Satellite's multiple organizations support.

Registering with an activation key

You can also register a system using an activation key from the organization. Activation keys will register systems to the organization in which the activation key was created. Activation keys are a good registration method to use if you want to allow users to register systems into an

organization without providing them login access to that organization:

```
rhnreg_ks --activationkey=21-myactivationkey
```

To move systems between organizations, the move can also be automated with scripts using the activation keys.

Note

The first few characters of the activation key are used to indicate the ID number of the organization that owns the key.

10.4. Users of an Organization

The **Users** page contains a list of all users on the Satellite, throughout all organizations.

The **Users** page lists the users assigned to the organization, including their real names, email address, and a check mark that indicates if the user is an Organization Administrator.

If you are the Organization Administrator, you can click the username to display the **User Details** page for the user.

Note

You must be logged in as the Organization Administrator to edit the User details for an organization. The Satellite Administrator role does not allow you to edit user details for organization users, it only allows you to assign the Satellite Administrator role to other users within the satellite.

10.5. Organizational Trusts

Organizations can share their resources with each other by establishing an organizational trust. Organizational trusts are defined by the Satellite Administrator and implemented by the Organization Administrator. Once a trust has been established between two or more organizations, the Organization Administrator from each organization is free to share as much or as little of their resources as they require. It is up to each Organization Administrator to determine what resources to share, and what shared resources from other organizations in the trust relationship to use.

Each individual relationship is unique and mutually exclusive from other trust relationships. For example, if the Accounting Organization trusts the Finance Organization, and the Finance Organization trusts the Facilities Organization, Accounting will not trust Facilities unless a separate trust relationship is defined between them.

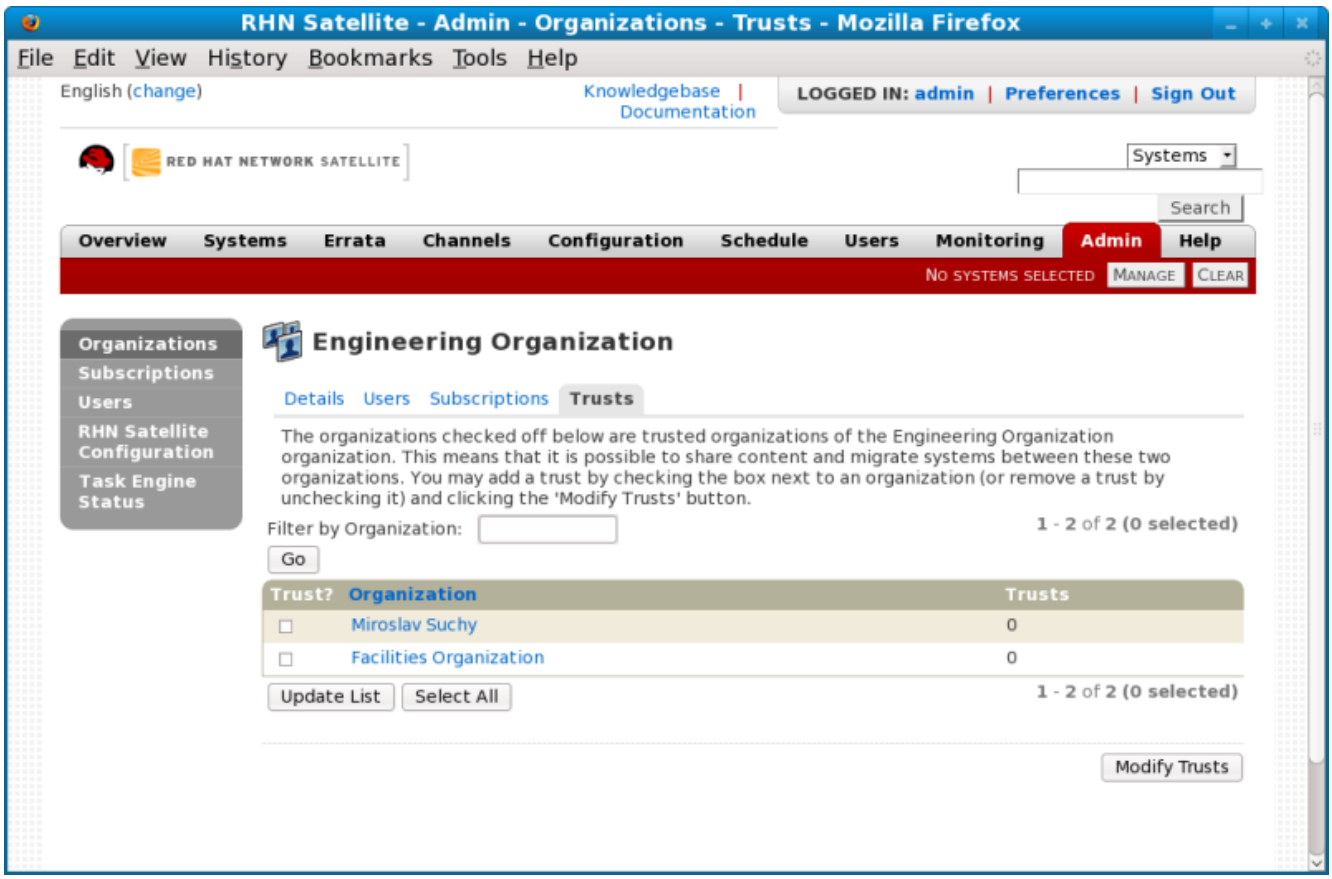
RHN Satellite - Admin - Organizations - Trusts - Mozilla Firefox
File Edit View History Bookmarks Tools Help
English (change)
Knowledgebase | Documentation
LOGGED IN: admin | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Monitoring Admin Help
NO SYSTEMS SELECTED MANAGE CLEAR
Organizations
Subscriptions
Users
RHN Satellite Configuration
Task Engine Status
Engineering Organization
Details Users Subscriptions Trusts
The organizations checked off below are trusted organizations of the Engineering Organization organization. This means that it is possible to share content and migrate systems between these two organizations. You may add a trust by checking the box next to an organization (or remove a trust by unchecking it) and clicking the 'Modify Trusts' button.
Filter by Organization:
1 - 2 of 2 (0 selected)
Go
Trust? Organization Trusts
Miroslav Suchy 0
Facilities Organization 0
Update List Select All
1 - 2 of 2 (0 selected)
Modify Trusts

Figure 10.3. Organizational Trusts

Procedure 10.2. Establishing an Organizational Trust

A Satellite Administrator can create a trust between two or more organizations. To do this, perform the following steps:

1. Select **Organizations** link on the menu on the **Admin** main page.
2. Click the name of one of the organizations and within the **Details** page, click the **Trusts** tab.
3. On the **Trusts** tab, there is a listing of all the other trusts on the RHN Satellite. If you have a long list of organizations, use the **Filter by Organization** text box to sort them.
4. Click the checkbox next to the names of the organizations you want to be in the organizational trust with the current organization.
5. Click the **Modify Trusts** button to create the trust.

Once an organizational trust has been established, organizations can share custom software channels with the other organizations in the trust. There are three levels of channel sharing that can be applied to each channel for access control:

Private

Make the channel private so that it cannot be accessed by any organizations except the owning organization.

Protected

Allow the channel to be accessed by specific trusted organizations of your choice.

Public

Allow all organizations within the trust to access the custom channel.

Trusted organizations that are granted access to the custom content using either protected or public access modes can allow their client systems to install and update packages from the shared channel. Subscription access can be lost when any of the following events occur:

- The Satellite Administrator removes the trust relationship
- The Organization Administrator changes channel access to private
- The Organization Administrator changes channel access to private and does not include the subscribed system's organization in the protected list
- The Organization Administrator deletes the shared channel directly
- The Organization Administrator deletes the parent channel of a shared child channel

Note

All Red Hat software channels are managed through entitlements. Organization Administrators cannot share Red Hat Channels because they are available to all organizations that have entitlements to those channels. The Satellite Administrator is responsible for assigning Red Hat software channel entitlements to each organization.

Procedure 10.3. Migrating Systems

In addition to sharing software channels, organizations in a trust can migrate systems to other trusted organizations by using the **migrate-system-profile** utility. The utility is executed from the command line, and uses ***systemID*** and ***orgID*** to specify the system migration and its destination organization. The Satellite Administrator can migrate a system from any trusted organization to any other in the trust. However, Organization Administrators can only migrate a system from their own organization to another in the trust.

The **migrate-system-profile** command requires the **spacewalk-utils** package to be installed, which is usually installed by default with RHN Satellite. When an organization migrates a system with the **migrate-system-profile** command, the system does not carry over any of the previous entitlements or channel subscriptions from the source organization. However, the system's history is preserved, and can be accessed by the new Organization Administrator in order to simplify the rest of the migration process, which includes subscribing to a base channel and granting entitlements.

1. Execute the command using the following format:

```
migrate-system-profile --satellite SATELLITE HOSTNAME OR IP --
systemId=SYSTEM ID --to-org-id=DESTINATION ORGANIZATION ID
```

For example, the Finance department (created as an organization in RHN Satellite with ***OrgID 2***) wants to migrate a workstation (with ***SystemID 10001020***) from the Engineering department, but the Finance Organization Administrator does not have shell access to the RHN Satellite server. The RHN Satellite hostname is **satserver.example.com**. The Finance Organization Administrator would type the following from a shell prompt:

```
migrate-system-profile --satellite satserver.example.com --systemId=10001020
--to-org-id=2
```

The utility then prompts for a username and password.

2. The system can then be viewed from the **Systems** page when logged into the RHN Satellite web interface. The migration process is completed by assigning a base channel and granting entitlements to the client for any other system registered to the organization, available from the system's **History** page in the **Events** tab.

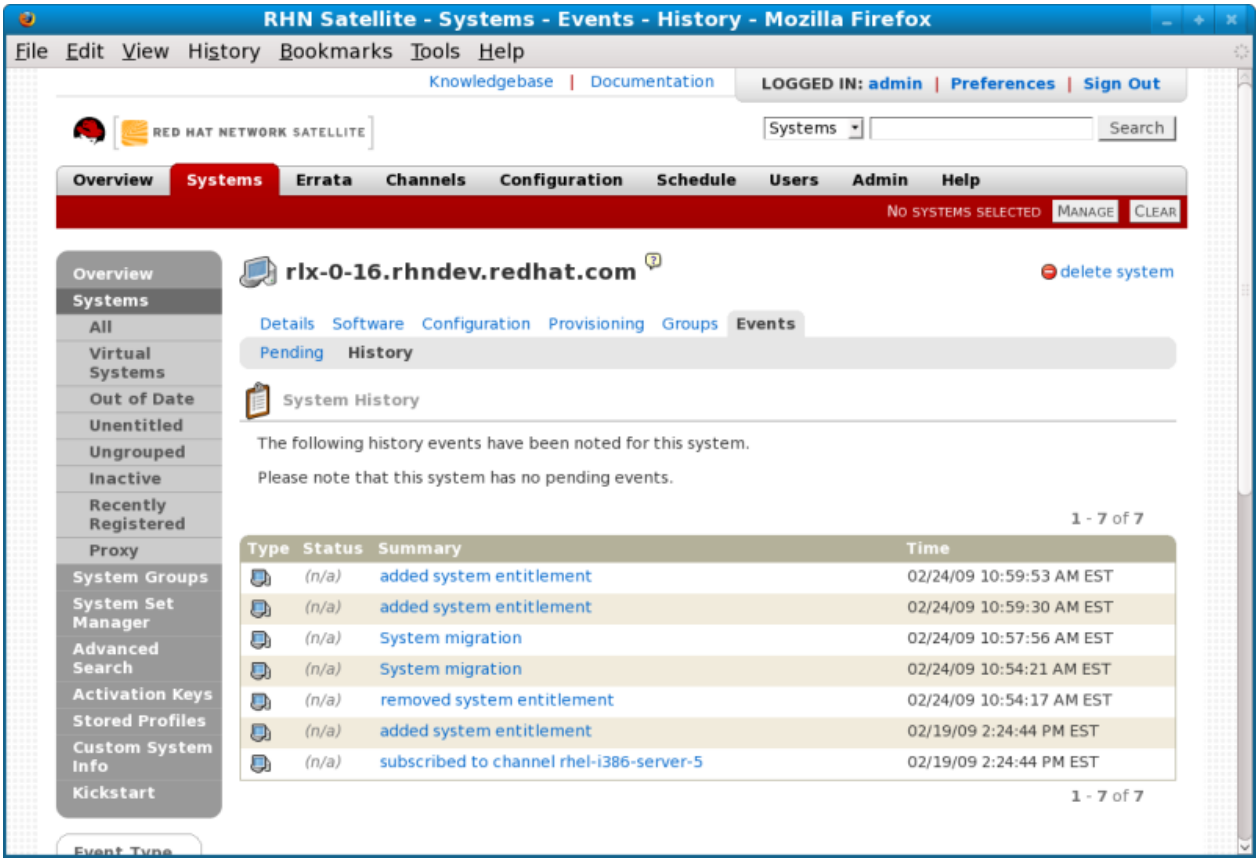
RHN Satellite - Systems - Events - History - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Knowledgebase | Documentation
LOGGED IN: admin | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Admin Help
No systems selected Manage Clear
Overview
Systems
All
Virtual Systems
Out of Date
Unentitled
Ungrouped
Inactive
Recently Registered
Proxy
System Groups
System Set Manager
Advanced Search
Activation Keys
Stored Profiles
Custom System Info
Kickstart
rlx-0-16.rhndev.redhat.com
delete system
Details Software Configuration Provisioning Groups Events
Pending History
System History
The following history events have been noted for this system.
Please note that this system has no pending events.
1 - 7 of 7
Type Status Summary Time
(n/a) added system entitlement 02/24/09 10:59:53 AM EST
(n/a) added system entitlement 02/24/09 10:59:30 AM EST
(n/a) System migration 02/24/09 10:57:56 AM EST
(n/a) System migration 02/24/09 10:54:21 AM EST
(n/a) removed system entitlement 02/24/09 10:54:17 AM EST
(n/a) added system entitlement 02/19/09 2:24:44 PM EST
(n/a) subscribed to channel rhel-i386-server-5 02/19/09 2:24:44 PM EST
1 - 7 of 7

Figure 10.4. System History

3. Satellite Administrators that need to migrate several systems at once can use the **--csv** option of **migrate-system-profile** to automate the process using a simple comma-separated list of systems to migrate.

   A line in the CSV file should contain the ID of the system to be migrated as well as destination organization's ID in the following format:

```
systemId,to-org-id
```

   The ***systemId***, for example could be **1000010000**, while the ***to-org-id*** could be **3**. An example CSV would look like the following:

```
1000010000,3
1000010020,1
1000010010,4
```

Revision History

Revision 3-5.400 **2013-10-31** **Rüdiger Landmann**
Rebuild with publican 4.0.0

Revision 3-5 **Wed Sept 19 2012** **Dan Macpherson**
Final packaging for 5.5

Revision 3-4 **Fri Aug 31 2012** **Athene Chan**
BZ#839798 Minor edit

Revision 3-3 **Fri Aug 24 2012** **Athene Chan**
BZ#839798 Changed 4.3 example to a standard format

Revision 3-3 **Fri Aug 24 2012** **Athene Chan**
BZ#839798 Changed 4.3 example to a standard format

Revision 3-2 **Fri Aug 24 2012** **Athene Chan**
BZ#826501 QA-reviewed changes applied.
BZ#884313 QA-reviewed changes applied.

Revision 3-1 **Fri Aug 17 2012** **Athene Chan**
BZ#848313 OpenSCAP chapter "How to View SCAP Results" added

Revision 3-0 **Thu Aug 9 2012** **Athene Chan**
Staging for Review

Revision 2-5 **Wed Aug 1 2012** **Athene Chan**
BZ#839798 Added spacewalk-clone-by-date chapter
BZ#826501 New OpenSCAP information added

Revision 2-0 **Fri Jul 6 2012** **Athene Chan**
Prepared for RHN Satellite 5.5 release
BZ#826501 Added OpenSCAP Chapter
OpenSCAP Screenshots added

Revision 1-5 **Mon Aug 15 2011** **Lana Brindley**
Folded z-stream release into y-stream

Revision 1-4 **Mon Jun 20 2011** **Lana Brindley**
BZ#701900 - PAM Authentication

Revision 1-3 **Mon Jun 20 2011** **Lana Brindley**
BZ#714029 - Fixed colour in image

Revision 1-2 **Wed Jun 15 2011** **Lana Brindley**
Prepared for publication

Revision 1-1 **Fri May 27 2011** **Lana Brindley**

Updates from translators

Revision 1-0 **Fri May 6, 2011** **Lana Brindley**
Prepare for translation

Revision 0-15 **Thu May 5, 2011** **Lana Brindley**
BZ#701818 - QE Review

Revision 0-14 **Mon May 2, 2011** **Lana Brindley**
BZ#248465 - QE Review

Revision 0-13 **Fri Apr 29, 2011** **Lana Brindley**
BZ#692295 - QE Review

Revision 0-12 **Mon Apr 18, 2011** **Lana Brindley**
BZ#691985 - Updating image

Revision 0-11 **Mon Apr 18, 2011** **Lana Brindley**
BZ#691990 - QE Review

Revision 0-10 **Mon Apr 18, 2011** **Lana Brindley**
BZ#691985 - QE Review

Revision 0-9 **Thu Apr 14, 2011** **Lana Brindley**
Technical review feedback

Revision 0-8 **Wed Apr 13, 2011** **Lana Brindley**
BZ#692314 - QE Review
BZ#692294 - QE Review
BZ#692291 - QE Review
BZ#692290 - QE Review
BZ#691988 - QE Review
BZ#691986 - QE Review
BZ#691981 - QE Review

Revision 0-7 **Wed Mar 23, 2011** **Lana Brindley**
Preparation for technical review

Revision 0-6 **Mon Feb 19, 2011** **Lana Brindley**
RPMs
Boot Devices
Organizations

Revision 0-5 **Fri Feb 18, 2011** **Lana Brindley**
Monitoring
PAM Authentication

Revision 0-4 **Mon Jan 10, 2011** **Lana Brindley**
Backup and Restore

Revision 0-3	**Fri Jan 7, 2011**	**Lana Brindley**
User Administration Preface Automatic Synchronization		
Revision 0-2	**Wed Jan 5, 2011**	**Lana Brindley**
User Administration		
Revision 0-1	**Tue Jan 4, 2011**	**Lana Brindley**
Completed new chapter structure		
Revision 0-0	**Tue Dec 21, 2010**	**Lana Brindley**
New document creation from original RHN Satellite Deployment Guide		

Index

A

add
- user, Adding, Deactivating, and Deleting User Accounts

API
- audit scans, Performing Audit Scans

audit scans, Performing Audit Scans
- OpenSCAP, Performing Audit Scans

auditing
- OpenSCAP, OpenSCAP

C

Cloning a Machine
- spacewalk-clone-by-date, Cloning a Machine

D

deactivate
- user, Adding, Deactivating, and Deleting User Accounts

delete
- user (RHN Satellite Server only), Adding, Deactivating, and Deleting User Accounts

E

email address
- changing, User Management

F

features, OpenSCAP Features

O

OpenSCAP, OpenSCAP, OpenSCAP Features, Prerequisites, Performing Audit Scans

P

PAM authentication
- implementation, PAM Authentication

password
- changing, User Management

Prerequisites
- OpenSCAP, Prerequisites

S

Satellite Administrator, User Management

spacewalk-clone-by-date, Cloning a Machine

U

user
- add, Adding, Deactivating, and Deleting User Accounts
- deactivate, Adding, Deactivating, and Deleting User Accounts
- delete (RHN Satellite Server only), Adding, Deactivating, and Deleting User Accounts

user roles, User Management

users, User Administration
- changing email address, User Management
- changing password, User Management
- roles, User Management

W

Web UI
- audit scans, Performing Audit Scans

website
- Users, User Administration